Configuring PPP Services

BayRS Version 13.00
Site Manager Software Version 7.00
BCC Version 4.05

Part No. 303537-A Rev 00
October 1998

Bay Networks

Where Information Flows.™

Bay Networks Where Information Flows.

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. October 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BayStack, BayStream, BCC, BCNX, BLNX, CLAM, SPEX, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product are Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xv
Text Conventions xvi
Acronyms xviii
Bay Networks Technical Publications xix
How to Get Help xx

Chapter 1
Starting PPP Services

Summary of PPP Services 1-2
Starting Configuration Tools 1-3
Adding or Modifying Interfaces for PPP 1-3
Starting PPP Services 1-4
Disabling and Reenabling PPP Services 1-5
Deleting PPP Services 1-6
Where to Go Next 1-7

Chapter 2
PPP Concepts

PPP Overview 2-2
Routing over a PPP Link 2-4
Initializing a PPP Interface 2-5
Establishing the PPP Link 2-5
Authenticating the PPP Link: PAP and CHAP 2-8
Password Authentication Protocol 2-8
Challenge Handshake Authentication Protocol 2-8
One-Way Authentication 2-9
Negotiating Network Layer Protocols 2-9
Datagram Encapsulation 2-10

PPP Dial Services Support 2-10
Dial-on-Demand 2-11
Bandwidth-on-Demand 2-11
Dial Backup 2-11
PPP Multiline 2-12
PPP Multilink 2-12
Using PPP Multilink 2-13
Multilink and Multiline Compatibility with Previous Versions 2-15
Configuring Multilink Operation 2-15
Balancing Traffic Loads 2-15
Using Multilink Fragmentation 2-16
Using Protocol Prioritization with Multiline and Multilink 2-17
Differences Between Multiline and Multilink 2-17
Monitoring PPP Link Quality 2-20
PPP Data Compression 2-22
Synchronous Versus Asynchronous Connections 2-23
Recognizing Asynchronous Modem Control Characters 2-23
PPP Line Parameters 2-24
Configuring IP to Run over PPP Interfaces 2-25
Detecting Loopback Conditions 2-25
PPP Interoperability 2-25
Stopping the Flow of Traffic over a PPP Interface 2-25
Where to Go Next 2-26

Chapter 3
Customizing PPP

Enabling PPP on an Interface 3-2
Setting Up Remote Addresses 3-4
Defining an IP Address for a Remote Peer 3-4
Defining an IPX Network Number and Node Number for a Remote Peer 3-5
Configuring AppleTalk 3-6
Defining a Remote AppleTalk Node Number for a Remote Peer 3-6
Defining the AppleTalk Routing Protocol 3-6
Enabling Bridging on an Interface 3-7
Enabling VINES Support on This Interface 3-8
Enabling DECnet IV Support on This Interface 3-9

Enabling Data Compression on This Interface 3-9
Enabling IPv6 on This Interface 3-10
Specifying the Type of Connection - PPP Mode 3-11
Configuring Multilink Fragmentation 3-12
Configuring Data Encryption 3-13
Disabling Network Control Protocols 3-13
Customizing PPP Lines 3-14
Editing PPP Line Parameters 3-15
Enabling Link Control on a Line 3-17
Setting Transmission Parameters 3-18
Setting the Restart Timer 3-18
Specifying the Interval Between Echo-Request Packets 3-19
Specifying the Acceptable Level of Echo-Reply Packet Loss 3-19
Specifying the Maximum Number of Configure-Request Packets 3-20
Specifying the Maximum Number of Terminate-Request Packets 3-21
Specifying the Maximum Configuration Failure Count 3-22
Setting a Time Limit for Convergence 3-23
Customizing PPP Authentication Parameters 3-24
Setting a Time Limit for Authentication 3-26
Customizing PAP 3-26
Specifying Local PAP Parameters 3-27
Specifying PAP Parameters for the Remote Peer 3-28
Allowing PAP Rejection 3-29
Customizing CHAP 3-29
Specifying the CHAP Secret 3-30
Specifying the CHAP Local Name 3-30
Specifying the CHAP Authentication Challenge Interval 3-30
Enabling PAP Fallback 3-30
Configuring PPP Interoperability with CLAM 3-31
Setting Up Link Quality Monitoring 3-31
Enabling Link Quality Monitoring and Reporting 3-32
Establishing the Timing of Link Quality Reports 3-32
Designating the Link Quality Report Timekeeper 3-32
Specifying the Link Quality Reporting Period 3-33
Specifying the Inbound Link Quality 3-33

Specifying the Outbound Link Quality 3-33
Summary Example for BCC Link Monitoring Commands 3-35
Specifying the Asynchronous Modem Control Character Map 3-36
Disabling Loopback Checking 3-38
Setting the Maximum Receive Unit (MRU) 3-39
Enabling RFC 1661 Compliance for Dial Circuits 3-41
Viewing Line Statistics for Multilink Circuits 3-42
Where to Go Next 3-44

Appendix A
PPP Parameters

PPP Interface Parameter Descriptions A-2
PPP Line Parameter Descriptions A-13

Appendix B
Default PPP Configuration

Appendix C
PPP Statistics

Appendix D
Monitoring PPP Using the BCC show Command

show ppp alerts D-2
show ppp bad-packets D-2
show ppp disabled D-2
show ppp enabled D-3
show ppp interfaces D-3
show ppp ip D-4
show ppp ipx D-4
show ppp ipx config D-4
show ppp ipx name-local D-5
show ppp ipx name-remote D-5
show ppp ipx negotiated D-6
show ppp line D-6
show ppp line async-map D-6
show ppp line config D-7
show ppp line params D-7

show ppp lqr D-8
show ppp lqr config D-8
show ppp lqr stats D-9

Index

Figures

Figure 2-1. Point-to-Point Network Connection 2-2
Figure 2-2. Initializing the PPP Interface 2-7
Figure 2-3. PPP-Encapsulated Frame 2-10
Figure 2-4. Multilink Circuit 2-14
Figure 2-5. Link Quality Monitoring from Router A's Perspective 2-21
Figure A-1. Site Manager PPP Interface Lists Window A-2
Figure A-2. Site Manager PPP Line Lists Window A-14

Tables

Table 1-1. PPP Configurable Functions 1-2
Table 2-1. Sample Data Link Control Protocol Options 2-3
Table 2-2. Network Control Protocols and Options 2-4
Table 2-3. Comparing Multiline and Multilink 2-18
Table 2-4. PPP Line Parameter Values 2-24
Table 3-1. PPP Modes 3-11
Table 3-2. PPP Line Parameters Configurable with the BCC 3-14
Table B-1. PPP Interface Parameters B-1
Table B-2. PPP Line Parameters B-2
Table C-1. PPP Statistics C-1

Preface

This guide describes PPP and what you do to start and customize PPP services on a Bay Networks® router.

You can use the Bay Command Console (BCC™) or Site Manager to configure PPP on a router. In this guide, you will find instructions for using both the BCC and Site Manager. If you choose to accept all the default parameters to start PPP on the router, you can use either BCC or Site Manager. If you choose to configure individual parameters, however, you will find that several parameters are not yet configurable with the BCC. In these cases, you must use Site Manager.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (see the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (see *Quick-Starting Routers*, *Configuring BayStack Remote Access*, or *Connecting ASN Routers to a Network)*.

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

You must also create and save a configuration file that contains at least one WAN interface, then retrieve the configuration file in local, remote, or dynamic mode. See *Configuring and Managing Routers with Site Manager*, depending on your platform, for information and instructions about the following topics:

- Initially configuring and saving a WAN interface
- Retrieving a configuration file
- Rebooting the device with a configuration file

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** <*ip_address*>, you enter: **ping 192.32.10.12**
bold text	Indicates text that you need to enter and command names and options. Example: Enter **show ip** {**alerts** | **routes**} Example: Use the **dinfo** command.
braces ({})	Indicate required elements in syntax descriptions where there is more than one option. You must choose only one of the options. Do not type the braces when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you must enter either: **show ip alerts** or **show ip routes**.

brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is: **show ip interfaces** [**-alerts**], you can enter either: **show ip interfaces** or **show ip interfaces -alerts**.
ellipsis points (. . .)	Indicate that you repeat the last element of the command as needed. Example: If the command syntax is: **ethernet/2/1** [<*parameter*> <*value*>] . . ., you enter **ethernet/2/1** and as many parameter-value pairs as needed.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** <*valid_route*> *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

BNCP	Bridge Network Control Protocol
BNX	Backbone Node Switch
BOFL	Breath of Life (message)
CCP	Compression Control Protocol
CHAP	Challenge Handshake Authentication Protocol
CRC	cyclic redundancy check
DNCP	DECnet Phase IV Control Protocol
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
HDLC	high-level data link control
HSSI	High-Speed Serial Interface
IP	Internet Protocol
IPCP	IP Control Protocol
IPX	Internetwork Packet Exchange
IPXCP	IPX Control Protocol
LAN	local area network
LCP	link control protocol
LQM	link quality monitoring
LQR	link quality report
MAC	media access control
MIB	Management Information Base
MTU	maximum transmission unit
NCP	network control protocol
OSI	Open Systems Interconnection
OSINLCP	OSI Network Layer Control Protocol
PAP	Password Authentication Protocol
RFC	Request for Comment

SMDS	Switched Multimegabit Data Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TFTP	Trivial File Transfer Protocol
VINES	Virtual Networking System
VNCP	VINES Network Control Protocol
WAN	wide area network
XNS	Xerox Network System
XNSCP	Xerox Network System Control Protocol

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
Starting PPP Services

PPP is a standard point-to-point protocol for sending data packets over serial (synchronous) and asynchronous lines.

This chapter describes how to create a basic PPP configuration by specifying values for required parameters only, and accepting default values for all other parameters of PPP.

Topic	Page
Summary of PPP Services	1-2
Starting Configuration Tools	1-3
Adding or Modifying Interfaces for PPP	1-3
Starting PPP Services	1-4
Disabling and Reenabling PPP Services	1-5
Deleting PPP Services	1-6
Where to Go Next	1-7

Summary of PPP Services

You can configure PPP to perform the functions shown in the following table. A check mark indicates whether you can configure a particular function with the tool shown at the top of the column.

Table 1-1. PPP Configurable Functions

Function	BCC	Site Manager
Route data over a PPP link	✓	✓
Perform data compression		✓
Run PPP over dial-up lines*	✓	✓
Run PPP over multiple lines		✓
Run PPP over a multilink circuit		✓
Set up protocol prioritization on a multiline circuit		✓
Configure IP to run over PPP interfaces	✓	✓
Enable and disable network control protocols	✓	✓
Use PPP with asynchronous modems		✓
Calculate and view line and circuit statistics		✓
Configure authentication protocols		✓
Set up link quality monitoring	✓	✓
Configure echo requests	✓	✓

* Dial backup only for BCC configuration

The following chapters describe how to do all these tasks. Chapter Chapter 2, "PPP Concepts," gives you detailed background information on PPP to help you make appropriate customizing choices. Chapter Chapter 3, "Customizing PPP," describes how to change the default settings after you configure the circuit.

Note: In examples, the text you enter appears in bold type.

Starting Configuration Tools

Before configuring PPP services, refer to the following user guides for instructions on how to start and use the Bay Networks configuration tool of your choice.

Configuration Tool	User Guide
Bay Command Console (BCC)	*Using the Bay Command Console (AN/BN Routers)*
Site Manager	*Configuring and Managing Routers with Site Manager*
NETarchitect	*Getting Started with Optivity Network Management System* *Configuring and Maintaining Networks with the NETarchitect System*

These guides also describe generically how to create or modify a device configuration and how to get help.

Adding or Modifying Interfaces for PPP

Before you can configure PPP-specific parameters, you must first configure at least one synchronous (SYNC) interface or high-speed serial interface (HSSI) that supports PPP as its WAN protocol. You must also configure the LAN protocol, usually IP, for that interface. The documents listed in the previous table describe how to add and modify these interfaces.

Starting PPP Services

When you add a PPP circuit, it is automatically enabled. To let data flow over this interface, you must also enable an upper-layer routing protocol (such as IP, IPX, or AppleTalk) to run on top of PPP. See the appropriate protocol-specific guides for information on these upper-layer protocols.

Note: The BCC supports only IP as the upper-layer protocol.

Using the BCC

To enable IP routing on a given interface, navigate to the IP prompt and enter:

state enable

For example, the following command enables IP routing on the interface with the IP address of 1.1.1.1.

```
ip/1.1.1.1# state enable
```

Using Site Manager

To enable IP routing over this PPP interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces**.	The Interfaces window opens.
3. Set **IP Enable** to **Enable**. (See page A-3.)	
4. Click on **OK** to accept the default values for all other PPP parameters.	The Configuration Manager window appears.

Disabling and Reenabling PPP Services

After changing certain PPP line parameters, you must force renegotiation of the link. To do this, you first disable, then reenable PPP on the link. Disabling the link also stops the flow of traffic from routing over the PPP interface, even though the upper-layer protocol may still be enabled.

Using the BCC

In BCC configuration mode, navigate to the PPP prompt for the interface and enter:

state disable

Then reenable PPP on the interface by entering:

state enable

For example, the following commands force renegotiation of the link by disabling, then reenabling PPP routing on the interface slot 3, circuit 1.

```
ppp/3/1# state disable
ppp/3/1# state enable
```

Using Site Manager

To force link renegotiation for this PPP interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces**.	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Enable (LCP)** to **Disable**. (See page A-14.)	
5. Click on **OK**.	The Interfaces window opens.
6. Set **Enable (LCP)** to **Enable**. (See page A-14.)	
7. Click on **OK**.	The Interfaces window appears.

Deleting PPP Services

You can delete PPP from a specific circuit by simply reconfiguring that circuit with a different configuration file that does not use PPP.

The way you delete PPP from *all* circuits on which it is currently configured depends on the tool you are using. For detailed information, refer to *Configuring and Managing Routers with Site Manager* or *Using the Bay Command Console*, as appropriate.

Caution: The BCC does not warn you before deleting objects.

Using the BCC

1. **To delete PPP from a circuit, navigate to the ppp prompt and type delete.**

   Deleting any object also deletes its subordinate objects.

   For example, the following command deletes PPP from the interface on slot 3, connector 1.

   ```
   ppp/3/1 delete
   ```

2. **To delete an interface (or other object), navigate to the prompt for that object and type delete.**

   For example, the following command deletes the synchronous interface on slot 3, connector 1.

   ```
   sync/3/1 delete
   ```

Using Site Manager

To use Site Manager to delete PPP from a circuit, do the steps in the following table.

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, click on the connector from which you want to delete PPP services.	The Edit Circuit window appears.
2. Click on **Done**.	The Configuration Manager window opens.
3. From the Protocols menu, choose **PPP**.	A menu showing additional options opens.
4. Click on **Delete PPP**.	Site Manager asks you to confirm your request for the deletion.
5. Click on **OK**.	Site Manager deletes PPP services from the circuit.

When you delete PPP globally, PPP no longer operates on the router. Be aware that the BCC software does not ask you to confirm your deletions.

Note: Site Manager does not let you delete PPP globally from a router running dial-on-demand, bandwidth-on-demand, or dial backup.

Where to Go Next

- Go to Chapter 2 to learn more about PPP concepts and characteristics.
- Go to Chapter 3 for instructions on how to customize a PPP interface.
- Go to Appendix A for a description of PPP parameters.
- Go to Appendix B for a list of PPP parameter default values.
- Go to Appendix C for a list of the PPP statistics that you can view.
- Go to Appendix D for descriptions of the BCC show commands for PPP.

Chapter 2
PPP Concepts

This chapter describes PPP concepts that can help you decide how to customize PPP parameters for your system. This chapter also addresses special configuration features of the Bay Networks implementation of PPP services. The following sections describe each of these items.

Topic	Page
PPP Overview	2-2
Routing over a PPP Link	2-4
Initializing a PPP Interface	2-5
Authenticating the PPP Link: PAP and CHAP	2-8
Negotiating Network Layer Protocols	2-9
Datagram Encapsulation	2-10
PPP Dial Services Support	2-10
PPP Multiline	2-12
PPP Multilink	2-12
Differences Between Multiline and Multilink	2-17
Monitoring PPP Link Quality	2-20
PPP Data Compression	2-22
Synchronous Versus Asynchronous Connections	2-23
Configuring IP to Run over PPP Interfaces	2-25
Detecting Loopback Conditions	2-25
PPP Interoperability	2-25
Stopping the Flow of Traffic over a PPP Interface	2-25
Where to Go Next	2-26

PPP Overview

Point-to-Point Protocol (PPP) is a standard method of routing or bridging datagrams between peer routers or other devices over serial point-to-point links (Figure 2-1).

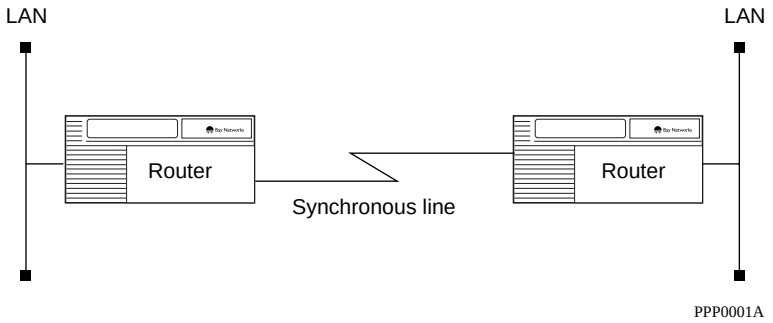


Figure 2-1. Point-to-Point Network Connection

PPP serves three major functions:

- Data link layer connection and management
- Network layer connection and management
- Datagram encapsulation

PPP uses a suite of data link and network control protocols to connect peer routers. PPP also allows peers to negotiate and determine data link and network layer options, such as those listed in Table 2-1 and Table 2-2. When negotiations complete successfully, PPP encapsulates the data and transmits it over the link.

Table 2-1. Sample Data Link Control Protocol Options

Option	Function
Maximum Receive Unit	Specifies the maximum receive unit (MRU) size for the line
Maximum Transmission Unit	Specifies the maximum transmission unit (MTU) size for the line
Authentication Protocol: • Password Authentication Protocol (PAP) • Challenge Handshake Authentication Protocol (CHAP)	Imposes network security by requiring an authentication process
Link Quality Protocol	Enables or disables link quality monitoring and reporting
Multilink Endpoint Discriminator	Enables the PPP multilink protocol and specifies the identity of the sender of the option

Table 2-2. Network Control Protocols and Options

Protocol	Negotiable Options
IP Control Protocol (IPCP)	IP Addresses (for backward compatibility), IP Address (default)
Internet Packet Exchange Control Protocol (IPXCP)	IPX Network Number, IPX Node Number, IPX Routing Protocol, IPX Router Name, IPX Configuration Complete
AppleTalk Control Protocol (ATCP)	AppleTalk Network Number, AppleTalk Node Number, AppleTalk Routing Protocol
DECnet Phase IV Control Protocol (DNCP)	None
OSI Network Layer Control Protocol (OSINLCP)	None
Xerox Networking System Control Protocol (XNSCP)	None
VINES Network Control Protocol (VNCP)	None
Bridge Network Control Protocol (BNCP)	MAC Type Selection

Routing over a PPP Link

You can enable the following protocols over PPP interfaces:

- AppleTalk
- DECnet Phase IV
- Internet Packet Exchange (IPX)
- Internet Protocol (IP)
- Open Systems Interconnection (OSI)
- Virtual Networking System (VINES)
- Xerox Network System (XNS)

The protocol that you selected when you first enabled PPP on the circuit is enabled by default. You can enable a different protocol by editing PPP protocol parameters, as described in Chapter 3.

Transparent/Translation Bridge and Source Route Bridge are other routing media that you can enable over any PPP interface. The PPP bridge accepts incoming traffic from any media (Ethernet, FDDI, token ring) and forwards data transparently (or translates when necessary).

Initializing a PPP Interface

PPP creates an interface between peer routers to allow them to exchange data. The routers initialize the interface in three phases:

1. Establishing the PPP link
2. Authenticating the link (optional for leased lines)
3. Negotiating network layer protocols

The following sections describe each phase.

Establishing the PPP Link

PPP's Link Control Protocol (LCP) helps establish a link. LCP generates three types of packets:

- Link configuration packets, including configure-request, configure-ACK, configure-NAK, and configure-reject packets
- Link termination packets, including terminate-request and terminate-ACK packets
- Link maintenance packets, including code-reject, protocol-reject, echo-request, and echo-reply packets

When two routers initialize a PPP dialogue, each of them sends a configure-request packet to the other (peer) router. Each configure-request packet contains a list of LCP options and corresponding values that the sending router uses to define its end of the link.

For example, a configure-request packet may specify the link's maximum transmission unit (MTU) size and whether the sender wants to use Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). The configure-request packet contains the user-configured values, which the sender and its peer router may need to negotiate.

Each router receives a configure-request packet from its peer. Each router responds with one of three types of packets:

- Configure-ACK

  If a router accepts the proposed LCP options, it responds with a configure acknowledgment (ACK) packet.

  When the routers on each side of the link send and receive configure-ACK packets, the LCP advances to an *open state*, which means that the PPP interface can advance to the next phase.

- Configure-reject

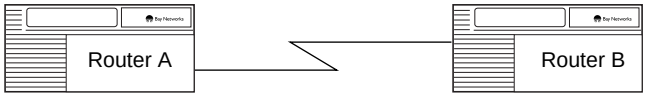
  If the configure-request packet contains options that the peer router is not willing to negotiate, the peer router sends back a configure-reject packet specifying the nonnegotiable options. From that point on, configure-request packets that the originating router sends should eliminate the unacceptable options.

- Configure-NAK

  If the peer disagrees with some or all of the values of the proposed options in the configure-request packet, it responds with a configure negative acknowledgment (NAK) packet. The configure-NAK packet notes the values that the peer disagrees with, and it includes the corresponding values that the peer would like to see in subsequent configure-request packets.

LCP negotiations between peers continue until either the routers converge (reach an agreement regarding the configure-request) and PPP advances to the next phase; until the peer router transmits a user-specified number of configure-NAK packets before sending a configure-reject packet; or until the configurable convergence timer expires. When the originating router receives a configure-reject packet, the originating router removes the offending options. The routers should then converge.

Figure 2-2 demonstrates how a PPP interface initializes.



1. PPP interface comes alive on network; begin LCP negotiations:

Send Configure-Request →
← Send Configure-Request
← Send Configure-ACK
Send Configure-ACK →

2. LCP opened; begin authentication phase, PAP or CHAP:

PAP*	**CHAP***
Send Authenticate-Request →	Challenge →
← Send Authenticate-ACK	← Response
	Response Match →

*Shows Router A initating authentication. Router B can also initiate authentication.

3. Authentication complete; begin NCP negotiations:

Send Configure-Request →
← Send Configure-Request
← Send Configure-ACK
Send Configure-ACK →

4. NCP open; begin transmitting data:

← **Send Data** →

PPP0002A

Figure 2-2. Initializing the PPP Interface

Authenticating the PPP Link: PAP and CHAP

In the authentication phase of PPP initialization, one or both peer routers enable either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Authentication is optional for leased lines but required for switched (dial-up) lines. You can optionally specify a time limit for authentication on switched lines.

Password Authentication Protocol

PAP imposes network security by requiring the peer router to send a PAP packet that contains a plain-text user identifier and password to the originating router before the interface can advance to the network layer protocol phase.

If PAP fails, the network administrator must change the identifier and password on both peer routers and disable and reenable LCP to reinitialize the line.

Challenge Handshake Authentication Protocol

CHAP imposes network security by requiring that the peers share a plain-text secret. The originating peer sends a challenge message to its receiving peer. The receiving peer responds with a value it calculates on the basis of knowing the secret. The first peer then matches the response against its own calculation of what the response should be. If the values match, it sends a success message, and the LCP establishes the link.

CHAP uses an incrementally changing identifier and a variable challenge value to provide network security. It also allows for repeated challenges at intervals that either router on a link can specify. A router may transmit challenge packets not only during the link establishment phase, but also at any time during the network layer protocol phase to ensure that the connection retains its integrity.

If CHAP fails, the network administrator must change the identifiers and secret on both peer routers and disable and reenable LCP to reinitialize the line.

Note: For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bringing up dial-on-demand, bandwidth-on-demand, and dial backup lines. Failure of either authentication protocol causes the connection to be dropped, without the network administrator’s intervention.

One-Way Authentication

One-way authentication uses an authentication protocol on only one side of a dial-up connection. The router placing the call disables the authentication protocol for a circuit, while the router on the receiving side enables authentication. Disabling the outbound authentication lets the router interoperate with other devices that may not allow two-way authentication or support CHAP.

The receiving router can use both PAP and CHAP in the same line pool. When the router receives a call, it authenticates using the user-configured protocol. If the calling router rejects the authentication protocol CHAP, the receiving router switches to PAP.

One-way authentication requires that PAP and CHAP be enabled in the same line pool. Set the PPP Local Authentication Protocol parameter to CHAP and enable PAP Fallback. You must also configure certain options for the switched circuit itself. See *Configuring Dial Services* for a description of how you must set up dial services to enable one-way authentication.

Negotiating Network Layer Protocols

PPP uses various network control protocols to determine the values of parameters during network layer negotiations, the final phase of PPP initialization. Like the LCP, each network control protocol allows peer routers to negotiate various network options over the data link by transmitting configure-request, configure-ACK, configure-NAK, and configure-reject packets.

Network options include which network addresses to use and which media types to bridge. Once both peer routers agree upon network options, the network control protocol reaches the open state. The routers then begin transmitting user data packets for any upper-layer protocols over the link.

Datagram Encapsulation

Before transmitting data across the link, PPP encapsulates data in a frame similar to a high-level data link control (HDLC) frame (Figure 2-3).

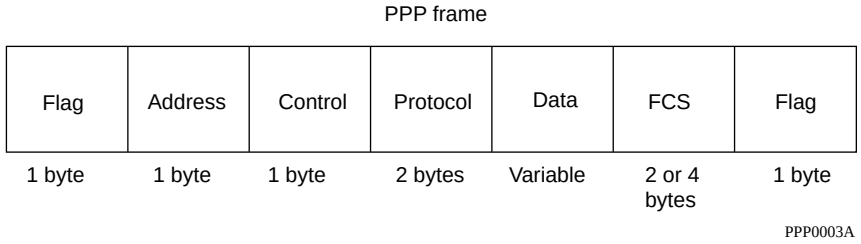


Figure 2-3. PPP-Encapsulated Frame

The parts of the PPP frame function as follows:

- The flag field marks the beginning and end of a frame. Peers on synchronous lines exchange flags continuously when there are no frames to transmit.
- The address field indicates which device originated the frame.
- The control field shows the frame type (information or administrative).
- The protocol field indicates the operative network layer protocol.
- The data field contains the data one link sends to the other. Its length is less than or equal to the MTU line size. The default maximum length is 1594 bytes; LCP negotiations determine the actual length.
- The frame check sequence (FCS) field shows the sequence order of the frame; router hardware computes the FCS. A 16- or 32-bit cyclic redundancy check (CRC) is at the end of each frame.

PPP Dial Services Support

Bay Networks dial services offer access to switched networks through dial-up line connections (also called *switched lines*) that are active only when you choose to use them. In contrast, a leased line is always available. If you transmit limited amounts of data, or if your data transmission is intermittent, dial services may let you run your network more effectively and economically.

PPP is automatically configured on lines that you select for dial services. PPP, with either CHAP or PAP, implements a router identification mechanism that dial services require.

Bay Networks provides three types of dial services: dial-on-demand, bandwidth-on-demand, and dial backup. For information on how to configure dial-on-demand, bandwidth-on-demand, and dial backup lines, see *Configuring Dial Services*.

Dial-on-Demand

Dial-on-demand enables you to establish a circuit “on demand” as opposed to having a leased-line connection, which is always available. By using a circuit on a demand basis, you can have a network connection only when you need it and significantly reduce your line costs.

Bandwidth-on-Demand

Bandwidth-on-demand uses secondary, dial-up lines to augment a primary, leased line (or lines) or an initial dial-on-demand line when the primary line experiences congestion. Congestion occurs when traffic volume exceeds the configured congestion threshold. Bandwidth-on-demand brings up these secondary lines one at a time, as needed, up to a maximum of 30 lines, including the primary lines. Up to 30 lines can be combined into a multilink bundle, depending upon platform constraints, total bundle speed, variance in member links speeds, and traffic characteristics. When congestion abates, the secondary lines become inactive.

Please consult the Bay Networks Technical Solutions Center in your area for design guidelines.

Dial Backup

If a primary PPP, frame relay, or standard line fails and you have enabled dial backup, the router automatically establishes a backup line and data transmission continues.

PPP Multiline

Bay Networks PPP services include support for the multiline feature, which lets you configure a single circuit that consists of one or more WAN data paths. A data path is a logical point-to-point channel that is a permanent (leased) line. Multiline provides both increased fault tolerance and greater bandwidth between two sites.

See the section "Differences Between Multiline and Multilink" on page 2-17 for a comparison of these features. For more information about the Bay Networks multiline feature, see *Configuring WAN Line Services* or *Configuring Ethernet, FDDI, and Token Ring Services*.

PPP Multilink

Note: BayStream software does not support the PPP multilink feature. If you use BayStream software, ignore this and the following sections relating to multilink.

The multilink feature of PPP provides capabilities beyond those of multiline circuits. The major characteristics of multilink include the ability to

- Use lines that have different speeds, proportionally distributing traffic over those lines
- Balance traffic load and maintain packet sequence
- Use switched lines (such as ISDN-B channels) as well as leased lines
- Monitor traffic volume

Configurations with bandwidth-on-demand, which can activate additional lines in response to increased traffic, can find these features particularly useful.

Multilink is available on all platforms that have more than one WAN line, including the following platforms:

- BLN®/BCN®
- AN®
- ASN™

Using PPP Multilink

The routers at each end of a PPP link (that is, a logical communications line) are called *peers*. A link is an individual communication channel between two peers. Typical links include one ISDN B channel, an aggregation of T1 DS0s, one dial-up modem connection, and one leased T1 line.

Links can be either leased or switched lines. All links must have the same data link encapsulation (PPP), and all links must have the same maximum transmission unit (MTU). On non-ISDN lines, you must configure the clock speed.

When you enable multilink, you can configure a set of links between two peers into a single "bundle," which can consist of up to 30 links, possibly of different bandwidths. (The practical maximum number of lines depends on factors such as the amount of memory, the number of lines configured, the speed of those lines, the packet sizes, and the traffic patterns.) With multilink configured, leased lines in a bundle can be on different router slots. Multilink distributes traffic over each logical line in a bundle in an amount roughly proportional to the effective bandwidth of the link.

With multilink and bandwidth-on-demand enabled, you can configure one side of the link as the congestion monitor. This router monitors network traffic and line usage. When the traffic exceeds a user-specified threshold, the bandwidth-on-demand monitor can bring up a secondary line.

Figure 2-4 shows a configuration that uses the multilink feature.

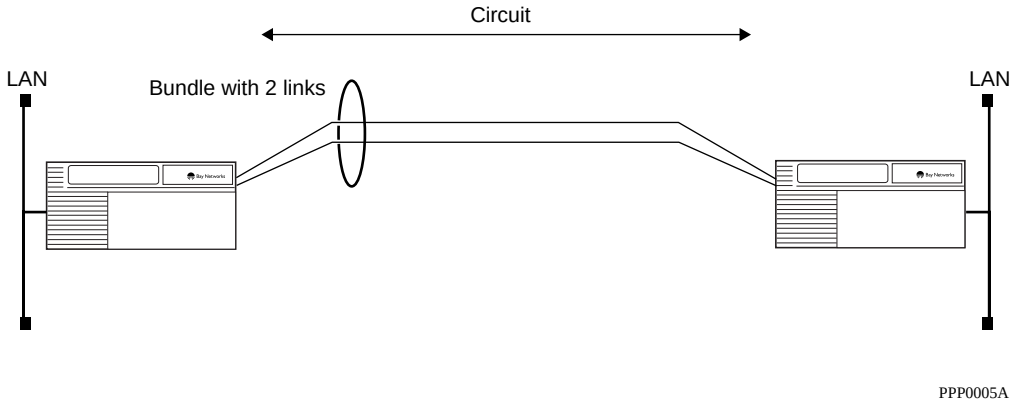


Figure 2-4. Multilink Circuit

As Figure 2-4 shows, a bundle is a logical connection between two routers. Once you have configured a circuit for multilink or bandwidth-on-demand operation, it always uses PPP multilink encapsulation.

All lines in a circuit must negotiate and perform multilink. You cannot pair non-multilink lines with multilink lines in a circuit. Multilink can resequence packets sent over different lines of the link. PPP supports packet fragmentation and reassembly, as described in the section "Using Multilink Fragmentation" on page 2-16.

You can use the multilink feature over the following physical media:

- V.35
- MCT1/MCE1
- ISDN-B channel drivers
- Raise-DTR modems
- V.25bis modems

Multilink and Multiline Compatibility with Previous Versions

A multi*line* circuit using PPP cannot communicate with a router running a router software version earlier than 9.0. Pre-9.0*x* versions use a multiline circuit with LCP running on only one line. In this situation, you must use uniline PPP.

A multi*link* circuit can communicate only with a router running Version 10.0 or later software (because earlier versions do not support the multilink feature). Attempting to run multilink on a pre-10.0 version results in the multilink circuit dropping back to multiline.

Configuring Multilink Operation

You configure a PPP multilink circuit by selecting the appropriate value in the PPP Mode parameter for the intended circuit. This parameter controls whether the local side of the bundle attempts to negotiate the multilink protocol, and whether the local circuit operates as the congestion monitor for bandwidth-on-demand. The congestion monitor locally monitors traffic congestion on the circuit. Only one side of any connection should be the congestion monitor.

Balancing Traffic Loads

In a configuration with multilink enabled, a sending router divides the outbound traffic among all the lines in the bundle. The configured external clock speed of each line determines the proportion of the total traffic each receives. For example, pairing a 9600-bit/second line with an ISDN B channel yields a clock-speed ratio of roughly 1:6.8, assuming same-size packets. That is, for every packet sent on the slower link, the router can send about seven packets on the faster link.

On the receiving end, multilink resequences packets arriving on different links using the sequence number from the multilink header. Gaps in the ordering may occur, however, when packets are corrupted or otherwise lost or when they arrive after packets with later sequence numbers. To minimize this situation, multilink buffers out-of-sequence packets in case the preceding sequence-numbered packets arrive shortly after the later-numbered packets.

Using Multilink Fragmentation

By default, PPP multilink allows packet fragmentation. With fragmentation enabled, PPP splits large datagrams into smaller packets and sends these packets across links in a multilink bundle. Enabling fragmentation means that PPP can split packets when necessary for better performance. PPP does not arbitrarily split all the packets it transmits. Fragmentation improves the distribution of data across multilink lines and uses buffer resources more efficiently, thereby improving the flow of data over multilink circuits. By default, multilink fragmentation is enabled. Bay Networks routers comply with RFC 1717, which defines PPP multilink.

Without multilink fragmentation, when PPP sends packets over a multilink bundle, it sends one packet over each line in sequence in a round-robin fashion. To optimize performance, PPP does attempt to send fewer packets on the slower lines. However, some packets with higher sequence numbers sent over faster lines *could* be received earlier than packets with lower sequence numbers sent over slower lines. Since PPP maintains the sequence of received packets, the receiving peer must store the out-of-sequence packets until the delayed packet arrives, and this can result in slower network performance. If the number of packets needing to be resequenced is greater than the available allowed buffer space, some packets could be considered late and discarded.

When you enable fragmentation, you can specify the minimum-size packet that you want PPP to consider fragmenting. (The default minimum size is 256 bytes.) Even with fragmentation enabled, PPP generally avoids splitting packets unless network performance considerations warrant it.

When necessary, PPP splits packets into fragments and then sends the fragments over the lines in the bundle, reassembling them on the receiving peer into the proper sequence. PPP discards all fragments of an incomplete reassembly. The number of fragments is equal to or less than the number of lines available. For bundles containing lines of different speeds, PPP tries to send the smaller fragments over the slower lines. This mechanism ensures a more even flow of data.

Packets sent over a multilink bundle have an outer header packet that contains a unique packet sequence number and allows for:

- Fragmentation of the original packets
- Assignment of sequence numbers to each fragment
- Transmission over a number of links in the bundle
- Reassembly of the original sequence and packet size at the receiving peer

Using Protocol Prioritization with Multiline and Multilink

When you configure a router, you can prioritize the different types of traffic sent across a synchronous line. This process is called *protocol prioritization.* The ability to prioritize traffic is important because some types of operations require faster responses than other types. For example, PPP control messages must have precedence over other types of data.

Selecting PPP on a circuit automatically enables protocol prioritization without specifying any filters.

With the multi*line* feature, you can configure both priorities and filters.

With the multi*link* feature, you can configure priority queuing. Priority queuing enables you to resequence outbound data packets into prioritized delivery queues called priority queues. To use priority queuing over multilink, first set the PPP Mode parameter to multilink and then configure the parameters in the Edit Protocol Priority Interface window. If compression is configured, the router prioritizes data before compressing it.

For more information about how to configure priority queuing and filters, see *Configuring Traffic Filters and Protocol Prioritization.*

Differences Between Multiline and Multilink

Both multiline and multilink use circuits consisting of one or more data paths between two peer routers. Each has its special characteristics and advantages, described in the following paragraphs and summarized in Table 2-3.

Table 2-3. Comparing Multiline and Multilink

Feature	Multiline	Multilink
Advantages	• Fault tolerance • Bandwidth availability	• Fault tolerance • Bandwidth availability • Uses all lines in the bundle for greatest speed and efficiency
Number of physical lines/ circuit	• Up to 31 concurrent data paths/group • Data paths can either be physical or logical lines (multiple independent data paths running over a single physical interface)	Up to 30 lines/bundle, depending on platform constraints, total bundle speed, variance in member links speeds, and traffic characteristics. Please consult the Bay Networks Technical Solutions Center in your area for design guidelines.
Grouped/bundled data paths	The data paths that together make up a multiline circuit must share the same speed, MTU, and encapsulation method.	Lines in a bundle can have different speeds.
Line types	Can use leased lines.	Can use leased as well as switched lines.
Protocol prioritization	• Automatically enabled • User can specify protocol prioritization and traffic filters	• Automatically enabled • User can specify protocol prioritization.
Used with these data link types	• Bay Networks standard synchronous • Frame relay direct mode • PPP	PPP (only)
Media supported	• Synchronous • T1/E1 • MCE1/MCT1 • HSSI	• Synchronous • T1/E1 • MCE1/MCT1 • ISDN B-channel drivers • Raise-DTR/V.25bis modems

(continued)

Table 2-3. Comparing Multiline and Multilink *(continued)*

Feature	Multiline	Multilink
Packet resequencing	Depends on the path selection: • With address-based selection (the default), packets always arrive in sequence. • With random path selection, packets traveling on different paths can arrive at their destination out of sequence.	Multilink maintains the sequence of packets sent over different lines of the link.
Support for bandwidth-on-demand	No	Yes
Miscellaneous	• Address-based selection does not always result in even traffic distribution across all data paths. • Random selection provides for even traffic distribution.	• All lines in a circuit must negotiate and perform multilink. • You cannot use nonmultilink lines in a circuit with multilink lines. • All data packets sent over a PPP multilink circuit travel as multilink packets.

Monitoring PPP Link Quality

To ensure that the router can successfully transfer data, PPP monitors the quality of the point-to-point link with link quality monitoring (LQM) and link quality report (LQR) packets. PPP supports LQM over standard synchronous interfaces only. PPP does not support LQM over high-speed serial interfaces (HSSI). BayStream software, however, *does* support LQM and LQR over HSSI interfaces.

Note: PPP uses LQM and LQR only if you set the Link Quality Protocol parameter to LINKQR. The default is None.

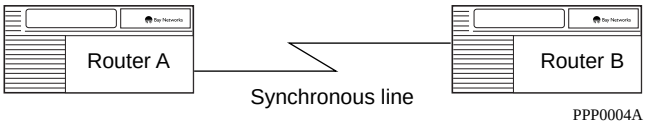
When you enable link quality monitoring through the Link Quality Protocol parameter, you are turning on monitoring only for the local router. For link quality monitoring to be operational, it only has to be enabled on one side of the link. If two routers are configured for different link quality reporting periods, they negotiate to the lower value, so that the LQR period will be the same on both sides of the link.

LQR packets contain counters of incoming and outgoing data packets for the routers on each side of the link. Each time a router receives an LQR packet, PPP uses that packet to calculate the outbound link quality (the percentage of packets the router transmitted that its peer successfully receives) and the inbound link quality (the percentage of packets that the peer transmitted that this router successfully receives).

After five LQR reporting periods, PPP averages the inbound and outbound link quality and compares these values against a user-specified threshold. This is a rolling average. After the first five LQR reporting periods, PPP acquires the data from the next period and drops the oldest data. Then it computes the link quality average for that set of five LQR periods, and so on.

If either the inbound or outbound link quality average drops below the threshold, PPP brings down the link. The driver software automatically brings the link back up and renegotiates the connection. PPP monitors the link control packets flowing over the connection and resumes network control protocol packet traffic when the link quality improves.

For example, in Figure 2-5, the acceptable outbound and inbound link quality configured on router A for the PPP interface is 100 percent. After five LQR periods, router A calculates the outbound and inbound link quality averages and determines that the inbound link quality average is below the 100 percent threshold (in this case, 90 percent). As a result, router A disables the link.



LQR Period	Packets Router A Transmitted	Packets Router B Received	Outbound Link Quality Router A
1	100	100	100%
2	100	100	100%
3	100	100	100%
4	100	100	100%
5	100	100	100%

Outbound average after 5 LQR periods = 100%

LQR Period	Packets Router A Received	Packets Router B Transmitted	Inbound Link Quality Router A
1	90	100	90%
2	90	100	90%
3	90	100	90%
4	90	100	90%
5	90	100	90%

Inbound average after 5 LQR periods = 90%

Figure 2-5. Link Quality Monitoring from Router A's Perspective

In addition to LQR packets, PPP periodically transmits echo-request packets (when echo-request is enabled). If the peer transmits a user-specified number of echo requests before receiving an echo reply from its peer router, the router disables the link and restarts.

Note: Echo-requests are disabled by default and are in no way related to link quality reporting.

PPP Data Compression

The Bay Networks data compression feature lets you reduce line costs and improve response times over wide area networks (WANs) running PPP.

Data compression eliminates redundancies in data streams. When you use compression on your network, bandwidth efficiency improves, and you can transmit more data over a given amount of network bandwidth.

Bay Networks data compression services for PPP include:

- Software-based compression (WCP and Hi/fn™ LZS®) for all platforms and all serial interfaces
- Hardware-based data compression for PPP networks that use the octal synchronous link module for the Backbone Node (BN®), using only FRE®-2 processors, and the FRE-2-060E processor module with the advanced compression coprocessor daughterboard.
- Hardware-based data compression for PPP networks that use the compression net module for the Access Stack Node (ASN).

You can use data compression on all PPP circuits, including multiline, multilink, bandwidth-on-demand, dial-on-demand, dial backup lines, and on ISDN BRI and PRI modules. You can use compression separately on each member of a multilink bundle. When you use compression on a bandwidth-on-demand, dial-on-demand, or dial backup circuit, the data compression feature automatically configures or deletes compression as lines are added to or removed from the circuit.

For complete descriptions of hardware and software data compression, descriptions of compression parameters, and instructions for configuring compression over a PPP interface, see *Configuring Data Compression Services*.

Synchronous Versus Asynchronous Connections

When you configure a dial (switched) circuit, you can specify whether you want transmission on that circuit to be synchronous or asynchronous. Switched services include dial-on-demand, bandwidth-on-demand, and dial backup. These function independently of the physical modem communication method.

In synchronous transmissions, the timing of each data transfer has a specific time relationship to the previous and next data transfer. Synchronous data transfers are fast because of the low network overhead relative to the amount of data transferred in each block, but they require more expensive, clock-driven data transmission equipment. In general, you might use synchronous data transmission for large data transfers.

Asynchronous communication, on the other hand, does not rely on a clock to define the beginning and end of a transmission. It uses lower-cost, asynchronous modems and appends a start and a stop bit to each transmission. This adds overhead to each data transfer, but it is often acceptable in lower-speed (less than 56KB, for example) and lower-volume data transfers. You can, for example, use an asynchronous modem connected to either a router or a PC to dial into a Bay Networks AN, ASN, BN, or BCN router or terminal server (such as a 5390) with asynchronous modem banks.

You configure most of the synchronous/asynchronous parameters when you set up dial services on a circuit and configure your modem pools. A modem pool can contain synchronous lines, asynchronous, or ISDN lines.

When you create or add a line to a dial services modem pool for a line configured to use PPP, the parameters that you must supply differ, depending on whether it is a synchronous or an asynchronous line. Refer to *Configuring Dial Services* for details on setting up and configuring both synchronous and asynchronous lines.

Recognizing Asynchronous Modem Control Characters

For a link that uses asynchronous modems, you can configure PPP to recognize and “escape” specified control characters that may occur in data packets. An example of such control characters is the XON/XOFF flow control mechanism that asynchronous modems use. The escape mechanism removes spurious control characters that external hardware may have introduced on the link.

During LCP negotiation, both peers negotiate the characters that they will recognize as modem control characters. PPP calculates and displays a map value based on this negotiation. Each end of the link maintains an asynchronous control character map for both sending and receiving.

When sending data, PPP inserts the escape character 0x7D in front of the control character and does a logical XOR operation, combining the control character with the value 0x20. When the receiving peer encounters these characters in the data stream, it strips off the escape character and converts the next character to the original asynchronous modem control character.

The async control character map consists of 32 bits. Each bit corresponds to one control character, 0x00 (the right end of the map) through 0x1F (the left end of the map); that is, 0 through 31, decimal. The actual map is a value used essentially as a mask. For example, the default map value, 0xA0000 (655360 decimal) allows the escaping of the control characters 0x11 (XON) and 0x13 (XOFF) if they occur in the data stream. Almost all modems need only this default value. The characters 0x7D and 0x7E are special characters that are always escaped in asynchronous data transmission. Chapter 3 describes how to build a customized async control character map.

PPP Line Parameters

When you enable PPP on a circuit (the default), PPP automatically sets the line parameters shown in Table 2-4. These parameters are the same for both synchronous and asynchronous connections.

Table 2-4. PPP Line Parameter Values

Parameter	Value
BOFL	Disable
Promiscuous	Enable
Service	Transparent
WAN Protocol	PPP

Depending on the configuration, you may have to specify explicitly certain other parameters. For more information on these parameters, refer to *Configuring and Managing Routers with Site Manager*, depending on your platform.

Configuring IP to Run over PPP Interfaces

When you enable numbered Internet Protocol (IP) support on a PPP interface, you must also configure an adjacent host entry for the peer router. See *Configuring IP Services* for instructions on configuring an adjacent host entry.

Detecting Loopback Conditions

As part of its network integrity checking, PPP tests for a loopback condition in which, effectively, it is talking to itself and not communicating with the network. Normally, you would want this feature enabled. For test purposes, however, you can disable this loopback detection feature by using the Technician Interface. After disabling this parameter, you must explicitly set it to Enable to reenable loopback checking. See "Disabling Loopback Checking" in Chapter 3 for instructions on how to set this parameter.

PPP Interoperability

The Bay Networks implementation of PPP conforms to the following RFCs: 1332, 1333, 1334, 1378, 1552, 1638, 1661, 1662, 1762, 1763, and 1764. Therefore, it can interoperate with routers that also conform to the same standards. If you have questions about whether a particular router can interoperate with your Bay Networks router running PPP, contact the Bay Networks Technical Solutions Center for your area, as listed in "About This Guide."

Stopping the Flow of Traffic over a PPP Interface

To stop traffic from routing over a PPP interface, either disable the Network Control Protocol (NCP) for the upper-level routing protocol or disable the upper-level protocol itself.

For example, if you disable the NCP for IP, even though IP is still enabled on the interface, it is no longer able to route traffic over the interface. See "Disabling Network Control Protocols" in Chapter 3 for instructions on disabling NCP parameters.

Disabling the routing protocol running on top of the PPP interface also automatically disables the NCP for the routing protocol. For example, if you disable IP on an interface, you disable the NCP for IP as well.

Where to Go Next

Go to Chapter 1 for instructions on how to start PPP on your router.

Go to Chapter 3 for instructions on how to customize a PPP interface.

Go to Appendix A for a description of PPP parameters.

Go to Appendix B for a list of PPP parameter default values.

Go to Appendix C for a list of the PPP statistics that you can view.

Go to Appendix D for descriptions of the BCC **show** commands for PPP.

Chapter 3
Customizing PPP

This chapter describes how to customize and enable PPP services. It assumes you have configured PPP on the interface using the default parameters, as described in Chapter 1, "Starting PPP Services and that you understand the PPP concepts in Chapter 2, "PPP Concepts. You should have read *Configuring and Managing Routers with Site Manager* or *Using the Bay Command Console*, as appropriate for your platform and the tool you are using. If you are using Site Manager, you should also have

1. Opened a configuration file
2. Specified router hardware, if this is a local mode configuration file
3. Selected the link or net module connector on which you are enabling PPP

You can enable PPP services most easily by accepting all the default parameter values. You do not have to configure any PPP parameters for PPP to run on your system.

If, however, you choose to change some or all of the default parameters, you'll find the information you need in this chapter. Site Manager lets you configure all of the PPP parameters; BCC lets you configure a subset of the PPP Line parameters. For a list of all PPP parameters, see Appendix A, "PPP Parameters."

Topic	Page
Enabling PPP on an Interface	3-2
Setting Up Remote Addresses	3-4
Enabling Bridging on an Interface	3-7
Enabling VINES Support on This Interface	3-8
Enabling DECnet IV Support on This Interface	3-9

Topic	Page
Enabling Data Compression on This Interface	3-9
Enabling IPv6 on This Interface	3-10
Specifying the Type of Connection - PPP Mode	3-11
Configuring Data Encryption	3-13
Disabling Network Control Protocols	3-13
Customizing PPP Lines	3-14
Editing PPP Line Parameters	3-15
Enabling Link Control on a Line	3-17
Setting Transmission Parameters	3-18
Customizing PPP Authentication Parameters	3-24
Setting Up Link Quality Monitoring	3-31
Specifying the Asynchronous Modem Control Character Map	3-36
Disabling Loopback Checking	3-38
Setting the Maximum Receive Unit (MRU)	3-39
Enabling RFC 1661 Compliance for Dial Circuits	3-41
Viewing Line Statistics for Multilink Circuits	3-42
Where to Go Next	3-44

Enabling PPP on an Interface

If you have already enabled PPP on the circuit that you want to configure, go to "Setting Up Remote Addresses" on page 3-4. If you haven't already done so, you must enable PPP on the interface. To do this, refer to Chapter 1, "Starting PPP Services."

By default, the protocol that you selected when you first configured this interface is enabled. If you want to enable a different protocol, you can do so as part of the customization. BCC supports only IP.

Using the BCC

To enable IP routing on a given interface, navigate to the IP prompt and enter:

state enable

For example, the following command enables IP routing on the interface with the IP address of 1.1.1.1.

```
ip/1.1.1.1# state enable
```

Using Site Manager

To enable IP routing over this PPP interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **IP Enable** to **Enable**. (See page A-3.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

The rest of this chapter describes how to configure and customize PPP for your system. Follow the instructions that apply to your network requirements.

Note: If you are using Site Manager and dynamically configuring a router that has already negotiated its Link Control Protocol, you must force LCP renegotiation on the interface to implement your changes. To do this, disable and then reenable the corresponding network control protocol(s).You can change as many parameters as you need to before forcing the renegotiation.

After making all your changes to any of the addressing or routing protocol enabling parameters:

1. **Set the corresponding network control protocol parameter (for example, IP Enable) to Disable and, if necessary, apply the changes.**
2. **Reset the same parameter to Enable and, if necessary, apply the changes.**

Refer to the description of enabling specific protocols for details.

Setting Up Remote Addresses

Using Site Manager, you can define an address and node number (depending on the requirements of the protocol you've chosen) that you want the remote peer to use. That is, you can define an

- IP address
- IPX network number and node number
- AppleTalk node number

depending on the protocol you enable. After enabling the protocol, specify the appropriate parameter(s) as described in the following sections.

Defining an IP Address for a Remote Peer

Use Site Manager to specify the IP address that the remote peer router should use. The interface you're configuring includes this address in its network control protocol (NCP) negotiations. The default is 0.0.0.0, indicating that this is an unnumbered interface. You can enter any valid IP address. (For information about unnumbered IP interfaces and on configuring an adjacent host entry, see *Configuring IP Services*.)

Beginning at the Configuration Manager window, complete the tasks in the following table to specify an IP address for a remote peer.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set the **Remote IP Address**. (See page A-8.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Defining an IPX Network Number and Node Number for a Remote Peer

Site Manager lets you specify an IPX network number and an IPX node number that you want the remote peer to use. The interface uses these numbers in its NCP negotiations.

Enter the IPX network number for the remote peer to use. There is no default value; you can enter any unique, valid, unreserved IPX network number, consisting of a string of up to eight hexadecimal characters. The value 0xffffffff is invalid.

The *negotiated* network number must be unique. It cannot be a previously assigned network number. Note that both sides of the link do not have to have the same network number; PPP negotiates the higher of the two numbers. In addition, the negotiated IPX network number can be 0 on both sides of the link. In this case, IPX defines the link's network number.

Be aware that the value for this parameter depends on the IPX configuration for this interface. For information about IPX and PPP interaction, refer to *Configuring IPX Services*.

If you want to specify an IPX node number for the remote peer to use, enter it here. The interface uses this IPX remote node number in its NCP negotiations.

To specify an IPX network number and remote node number, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set the **IPX Network Number**. (See page A-8.)	
4. Set the **IPX Remote Node Number**. (See page A-9.)	
5. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Configuring AppleTalk

To enable AppleTalk on the interface, use Site Manager to configure an AppleTalk node number and the AppleTalk routing update protocol for the remote peer to use.

Defining a Remote AppleTalk Node Number for a Remote Peer

If you want to specify an AppleTalk node number that the peer router should use, enter it here. There is no default value; you can enter any valid AppleTalk node number. This interface includes this AppleTalk node number in its network control protocol negotiations.

Defining the AppleTalk Routing Protocol

You can specify the AppleTalk routing update protocol for the peer router to use. Since the only option for the AppleTalk Routing Protocol is the Routing Table Management Protocol (RTMP), you can simply accept the default value. This interface specifies AppleTalk RTMP as the routing update protocol in NCP negotiations.

To specify an AppleTalk Node Number and the AppleTalk Routing Protocol, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set the **Remote AppleTalk Node**. (See page A-9.)	
4. Set the **AppleTalk Routing Protocol**. (See page A-10.)	
5. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Enabling Bridging on an Interface

When bridging is enabled for an interface, PPP accepts bridged traffic in the specified encapsulation and forwards it over the PPP network. Site Manager lets you enable or disable bridging for Ethernet, FDDI, and/or token ring encapsulated packets. By default, all these parameters are enabled. If you change any of these parameters dynamically (that is, for a router that has already completed its negotiations), you must force LCP renegotiation on the interface, as previously described.

Before you can enable a particular type of encapsulated bridged traffic, you must enable bridging on the interface. You do this by default if you enabled bridging when you initially set up the PPP interface, but you can disable or re-enable it here. To stop traffic from being bridged over this interface, set this parameter to Disable.

The Bridge Enable parameter enables or disables the network control protocol for the bridge. It does *not* enable or disable bridging services for the interface. However, disabling the network control protocol for the bridge stops traffic from being bridged over this interface.

With the bridging feature enabled, you can then enable or disable bridging for particular encapsulation types. For example, if you want PPP to accept and forward Ethernet-encapsulated bridged traffic, set the Bridge Ethernet parameter to Enable (the default).

To enable or disable bridging on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **Bridge Enable**. (See page A-6.)	

Site Manager Procedure	
You do this	**System responds**
4. Enable or disable the encapsulation mode for the type of traffic bridged on this interface. • Set **Bridge Ethernet** (See page A-10.) • Set **Bridge FDDI**. (See page A-11.) • Set **Bridge Token Ring**. (See page A-11.)	
5. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Enabling VINES Support on This Interface

If you enabled VINES support when you first configured PPP on this interface, this parameter defaults to Enable; otherwise, the default is Disable. To stop VINES traffic from being routed over this interface, set this parameter to Disable.

This parameter enables or disables the network control protocol for VINES. It does not enable or disable VINES routing services for the interface. However, disabling the network control protocol for VINES stops VINES traffic from being routed over this interface.

To enable or disable VINES support on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **VINES Enable**. (See page A-6.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Enabling DECnet IV Support on This Interface

If you enabled DECnet IV support when you first configured PPP on this interface, the DECnet IV Enable parameter defaults to Enable; otherwise, the default is Disable. To stop DECnet IV traffic from being routed over this interface, set this parameter to Disable. This parameter enables or disables the network control protocol for DECnet IV. It does not enable or disable DECnet IV routing services for the interface. However, disabling the network control protocol for DECnet IV stops DECnet IV traffic from being routed over this interface.

To enable or disable DECnet IV traffic on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **DECnet IV Enable**. (See page A-4.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Enabling Data Compression on This Interface

If you enabled data compression when you initially configured this interface, then data compression is configured by default for PPP; otherwise, the default is Disable. To stop compression over this interface, set this parameter to Disable.

This parameter allows or stops data compression. It does not enable or disable data compression for the interface, but disabling the Compression Control Protocol (CCP) stops data compression over this interface.

To enable or disable data compression on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **CCP Enable**. (See page A-7.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Enabling IPv6 on This Interface

If you enabled Internet Protocol, version 6 (IPv6) support when you initially configured this interface, then the IPV6 parameter is enabled by default for PPP; otherwise, the default is Disable. To stop IPv6 traffic from being routed over this interface, set this parameter to Disable.

This parameter enables or disables the network control protocol for IPv6. It does not enable or disable IPv6 routing services for the interface. However, disabling the network control protocol for IPv6 stops IPv6 traffic from being routed over this interface.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **IPV6 Enable**. (See page A-7.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Specifying the Type of Connection - PPP Mode

The PPP Mode parameter indicates the type of connection on this interface: single-line, multiline, multilink, or multilink monitor. Your choice of options depends on the type of circuit you are configuring. This section deals with how you use Site Manager to configure each of these PPP modes.

Table 3-1 compares the various PPP modes.

Table 3-1. PPP Modes

Connection Type	PPP Mode Value	Comments
Any nonmulitlink circuit	Normal	This is the default value for any nonmultilink connection.
Multiline	Normal	Same as single-line connection.
Multilink	Multilink or Monitor	• Set the PPP Mode parameter to Multilink to configure the circuit for multilink operation. • Set it to Monitor if you want the local router to serve as the congestion monitor for the multilink circuit. Only one side of any connection should be the monitor.

For a description of the differences between multiline and multilink connections, see "Differences Between Multiline and Multilink" in Chapter 2. For more information about multiline connections, see *Configuring Dial Services*.

To configure the PPP mode on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **PPP Mode**. (See page A-12.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Configuring Multilink Fragmentation

For multilink circuits that include different speed links and that may carry both large and small packets, you can optionally enable multilink fragmentation. PPP fragments packets only if doing so will improve the flow of data over the circuit. When necessary, PPP splits packets into encapsulated fragments and then sends the fragments over the lines in the multilink bundle, reassembling them on the receiving peer into the proper sequence. PPP discards all fragments of an incomplete reassembly. The number of fragments is always equal to or less than the number of lines in the bundle. Multilink fragmentation is enabled by default.

When you enable fragmentation, you can specify the minimum size packet that you want PPP to consider fragmenting. The default minimum size is 256 bytes.

To configure the multilink fragmentation and minimum fragment size on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **Multilink Fragmentation**. (See page A-12.)	
4. Set **Fragmentation Trigger Size**. (See page A-13.)	
5. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Configuring Data Encryption

Bay Networks offers software-based data encryption services for PPP dedicated links for the BN®, AN®, ARN™, ASN™, System 5000 router modules, and all serial interfaces. This includes encryption on multiline and multilink circuits. If you configure data encryption on a PPP circuit, the encryption parameter fields (Mode Protection Key, Encrypt Enable, LTSS Name, and LTSS Value) on the PPP Interface Lists window are filled in. Otherwise, these fields are inactive. While you can change these parameters through the PPP Interface Lists window, they are only part of a suite of encryption parameters, and any changes you make can have significant effects on the entire encryption process. Therefore, before changing any of these encryption parameters, please see *Configuring Data Encryption Services* for a full description of all the available data encryption parameters.

Disabling Network Control Protocols

To stop traffic from routing over a PPP interface, either

- Disable the NCP for the upper-level routing protocol.

  For example, if you disable the NCP for IP (by setting the IP Enable parameter to Disable), even though IP is still enabled on the interface, it is no longer able to route traffic over the interface.

- Disable the upper-level routing protocol itself.

  If you disable the routing protocol running on top of the PPP interface, you also automatically disable the NCP for the routing protocol. For example, disabling IP on an interface disables the NCP for IP as well.

Using the BCC

Navigate to the IP prompt and enter

state disable

For example, the following command disables IP routing on the interface with the IP address of 1.1.1.1.

```
ip/1.1.1.1# state disable
```

Using Site Manager

To stop traffic from routing over this PPP interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **IP Enable** to **Disable**. (See page A-3.)	
4. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window appears.

Customizing PPP Lines

The PPP line parameters specify the characteristics of individual lines within the interface. You can edit the default PPP line parameter values to fit your particular system requirements. Appendix Appendix B, “Default PPP Configuration lists the default PPP line parameter values. The following sections describe how to customize those parameters.

You can configure or modify all the PPP line parameters using Site Manager, but only a subset using the BCC. Table 3-2 lists the PPP line parameters that you can modify using BCC commands.

Table 3-2. PPP Line Parameters Configurable with the BCC

Site Manager Parameter Name	BCC Parameter
Restart Timer in Seconds	restart-timer
Seconds between Xmit of Echo-Request	echo-requests
Echo-Reply Acceptable Loss	echo-replies lost
Max Configure-Requests	max-configure-requests
Max Terminate-Requests	max-terminate-requests
Max Configuration Failure Count	max-configure-fails
Link Quality Protocol	link-quality-protocol

(continued)

Table 3-2. PPP Line Parameters Configurable with the BCC *(continued)*

Site Manager Parameter Name	BCC Parameter
Peer Link Quality Report Timer	peer-lqr-timer
LQR Reporting Period	lqr-reporting-period
Inbound Link Quality	lqr-percentage-received
Outbound Link Quality	lqr-percentage-sent
Magic Num Disable	magic-number

Editing PPP Line Parameters

If you change any of the parameters in the following list and you are dynamically configuring a router that has already negotiated its link control protocol (LCP), you must force link (that is, LCP) renegotiation on the interface to implement your changes.

- Echo-Reply Acceptable Loss
- Max Configure-Requests
- Max Terminate-Requests
- Max Configuration Failure Count
- Local Authentication Protocol
- Local PAP ID
- Local PAP Password
- Remote PAP ID
- Remote PAP Password
- Link Quality Protocol
- Peer Link Quality Report Timer
- LQR Reporting Period
- CHAP Secret
- CHAP Local Name
- CHAP Periodic Timer
- Asynchronous Control Character Map

- Authentication Timer
- Convergence Timer
- Magic Num Disable

Using the BCC

To force LCP negotiation using the BCC, navigate to the ppp prompt and enter:

state disable

then enter

state enable

For example, the following commands force LCP renegotiation on interface 3/1 by first disabling, then reenabling PPP.

```
ppp/3/1# state disable
ppp/3/1# state enable
```

Using Site Manager

Disable and then reenable the Enable (LCP) parameter. You can change as many parameters as necessary before forcing the renegotiation. After making all your changes to these parameters:

1. **Set the Enable (LCP) parameter to Disable and, if necessary, apply the changes.**
2. **Reset the Enable (LCP) parameter to Enable and, if necessary, apply the changes.**

To force link renegotiation on this PPP interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Set **Enable (LCP)** to **Disable**. (See page A-14.)	
5. Click on **OK**.	The Interfaces window opens.
6. Choose **Lines**.	The Lines window opens.
7. Set **Enable (LCP)** to **Enable**. (See page A-14.)	
8. Click on **OK**.	The Interfaces window opens.

Enabling Link Control on a Line

The link control protocol (LCP) is enabled by default on the interface. Disabling the Enable (LCP) parameter generates a “close” event to the LCP, and enabling this event generates an “open” event to the LCP. A major use of this sequence is to force LCP renegotiation on the interface during dynamic reconfiguration. Doing so means that any changes you have made to the line parameters are included in the negotiations.

To enable the link control protocol on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Enable (LCP)**. (See page A-14.)	
5. Click on **OK**.	The Interfaces window opens.

To disable LCP on this interface, set Enable (LCP) parameter to Disable. To reenable LCP, set this parameter to Enable.

Setting Transmission Parameters

You can specify the timing of transmissions and the threshold for considering the link to be down using the parameters described in the following sections.

Setting the Restart Timer

The value of the Restart Timer in Seconds parameter specifies the number of seconds that the restart timer waits before retransmitting data. The default value is 3 seconds, and the range is 1 through 1000 seconds.

Using the BCC

Navigate to the line prompt for the circuit and enter

restart-timer *seconds*

For example, the following command sets the restart timer to wait 5 seconds before retransmitting data on circuit 3/1.

```
line/3/1# restart-timer 5
```

Using Site Manager

To set the restart timer on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Restart Timer in Seconds**. (See page A-15.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Specifying the Interval Between Echo-Request Packets

The value of the Seconds between Xmit of Echo-Request parameter specifies the number of seconds that the router waits between the transmission of echo-request packets. A value of 0 (the default) means that this parameter is turned off.

Using the BCC

Navigate to the line prompt for the circuit and enter

echo-requests *seconds*

For example, the following command sets the echo-request interval to 5 seconds on circuit 3/1.

```
line/3/1# echo-requests 5
```

Using Site Manager

To set the interval between transmissions of echo-request packets on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Seconds between Xmit of Echo-Request**. (See page A-15.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Specifying the Acceptable Level of Echo-Reply Packet Loss

The Echo-Reply Acceptable Loss parameter specifies the maximum number of unacknowledged echo-request packets that the router will transmit before declaring the point-to-point link down. The default value is 3 packets.

Using the BCC

Navigate to the line prompt for the circuit and enter

echo-replies-lost *seconds*

For example, the following command sets the number of acceptable packets lost to 5 seconds on circuit 3/1.

```
line/3/1# echo-replies-lost 5
```

Using Site Manager

To set the interval between transmissions of echo-request packets on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Echo-Reply Acceptable Loss**. (See page A-15.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Specifying the Maximum Number of Configure-Request Packets

The Max Configure-Requests parameter specifies the maximum number of unacknowledged configure-request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond. The link is then brought down. Valid acknowledgments include configure-ACK, configure-NAK, or configure-reject packets. The default value is 10 packets.

Using the BCC

Navigate to the line prompt for the circuit and enter

max-configure-requests *seconds*

For example, the following command sets the maximum number of unacknowledged configure-request packets allowed to 5 on circuit 3/1.

```
line/3/1# max-configure-requests 5
```

Using Site Manager

To set the maximum number of unacknowledged configure-request packets allowed on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Max Configure-Requests**. (See page A-16.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Specifying the Maximum Number of Terminate-Request Packets

PPP uses the Maximum Terminate-Requests parameter to specify the maximum number of unacknowledged terminate-request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond. The valid acknowledgment is a terminate-ACK packet. The default value is 2 packets.

Using the BCC

Navigate to the line prompt for the interface and enter

max-terminate-requests *seconds*

For example, the following command sets the maximum number of unacknowledged terminate-request packets allowed to 5 on interface 3/1.

```
line/3/1# max-terminate-requests 5
```

Using Site Manager

To set the maximum number of unacknowledged terminate-request packets allowed on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Max Terminate-Requests**. (See page A-16.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Specifying the Maximum Configuration Failure Count

The Max Configuration Failure Count parameter specifies the maximum number of configure-NAK packets that the router sends before sending a configure-reject packet for those options that it does not agree with. The default value is 10 packets.

Using the BCC

Navigate to the line prompt for the interface and enter

max-configure-fails *seconds*

For example, the following command sets the maximum number of configure-NAK packets allowed to 5 on interface 3/1.

```
line/3/1# max-configure-fails 5
```

Using Site Manager

To set the maximum number of configure-NAK packets allowed on this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Max Configuration Failure Count**. (See page A-17.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Setting a Time Limit for Convergence

Convergence occurs when the peers have negotiated all the parameters needed to establish a dial services connection. You can limit the amount of time that PPP attempts to negotiate a switched PPP interface by setting the Convergence Timer parameter.

This parameter applies only to a switched PPP interface. The convergence timer specifies the maximum number of seconds allowed for the completed negotiations. It limits the LCP negotiations and requires at least one NCP to negotiate within the configured amount of time. The default value is 300 seconds. If the timer expires before the negotiation completes, the connection is dropped.

The convergence timer allots the configured number of seconds for the LCP to negotiate and allots the same period for one NCP to complete negotiations.

Using the BCC

The BCC does not allow you to configure this parameter.

Using Site Manager

To set the maximum time allowable for convergence for this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Convergence Timer**. (See page A-27.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Customizing PPP Authentication Parameters

PPP imposes network security by offering support for two types of authentication protocols: Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP).

Site Manager lets you configure the PPP authentication parameters; the BCC does not. The following sections describe how to configure PPP to implement PAP and CHAP.

Note: For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bring up demand, backup, and bandwidth lines. You must configure the CHAP local name, CHAP secret, PAP ID, and PAP password through the Dial menu. See *Configuring Dial Services* for details.

In addition, for all dial services, failure of either authentication protocol causes the connection to be dropped, and no intervention from the network administrator is needed.

For leased lines, the authentication phase is optional.

You must first specify what, if any, local authentication protocol this interface uses. The Local Authentication Protocol parameter specifies the type of authentication protocol that this interface uses: None, PAP, or CHAP.

If you do not want to enable security features on this interface, accept the default, None.

To enable Password Authentication Protocol, select PAPAUTH. Then define the Local PAP ID and Local PAP Password parameters for this interface.

To enable Challenge Handshake Authentication Protocol, select CHAP. Then define the CHAP Secret, CHAP Local Name, and CHAP Periodic Timer parameters for this interface.

Using the BCC

The BCC does not allow you to configure this parameter.

Using Site Manager

To set the local authentication protocol for this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Local Authentication Protocol**. (See page A-18.)	
5. If you specified • **None**, continue with the next step in this table. • **PAPAUTH or CHAP**, continue with "Setting a Time Limit for Authentication" on page 3-26.	
6. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Setting a Time Limit for Authentication

You can specify the maximum number of seconds the router waits for a response to its authentication messages by setting the Authentication Timer parameter. If the timer expires before the negotiation completes, the router drops the connection. The default value is 10 seconds.

Using the BCC

The BCC does not allow you to configure this parameter.

Using Site Manager

To set a time limit for this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Authentication Timer**. (See page A-27.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Customizing PAP

When PAP is the authentication protocol, you must also specify a local PAP ID, a local PAP password, and a remote PAP ID and remote PAP password for the peer. During the authentication phase of link creation, PPP uses these parameters to verify the peer's right to communicate with the local router.

Note: For dial services that use PAP, you must configure the local PAP ID, the local PAP password, the remote PAP ID, and the remote PAP password through the Dial menu. See *Configuring Dial Services* for details.

Specifying Local PAP Parameters

If you did not enable PAP on the local peer, ignore the local PAP parameters that follow. If you set the local authentication protocol to PAPAUTH, specify a unique local PAP identifier and local PAP password for this interface.

During the interface's authentication phase, all password authenticate-request messages the peer router sends to this interface must include the correct PAP ID and PAP password. Otherwise, the interface sends an authenticate-NAK message and the link is not created.

The Local PAP ID parameter specifies the identifier assigned to this interface. The identifier can consist of any text string, up to 25 characters long. There is no default value.

The Local PAP Password parameter specifies the password assigned to this interface. The password can consist of any text string, up to 25 characters long. There is no default value.

Using the BCC

The BCC does not allow you to configure these parameters.

Using Site Manager

To set a local PAP identifier and local PAP password for this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Local PAP ID**. (See page A-19.)	
5. Set **Local PAP Password**. (See page A-19.)	
6. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Specifying PAP Parameters for the Remote Peer

If the remote peer does not have PAP enabled, ignore the remote PAP parameters that follow.

During the authentication phase of link creation, PPP uses the remote PAP ID and remote password to verify the local peer's right to communicate with the remote router. During the authentication phase, this interface must include the correct remote PAP ID and remote PAP password in all password authenticate-request messages it sends to the local peer router; otherwise, the peer router sends an authenticate-NAK message and the link is not created.

If the remote peer has PAP enabled, specify the Remote PAP ID parameter, which assigns a PAP identifier to the remote peer. There is no default value.

The Remote PAP Password parameter specifies the password assigned to the remote peer router. The password can consist of any text string, up to 25 characters long. There is no default value.

Using the BCC

The BCC does not allow you to configure these parameters.

Using Site Manager

To set a PAP identifier and PAP password for the remote peer of this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Remote PAP ID**. (See page A-20.)	
5. Set **Remote PAP Password**. (See page A-20.)	
6. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Allowing PAP Rejection

Some peers do not use PAP. If you set the Allow PAP Reject parameter to Enable, your router accepts the Reject message from such a peer and removes PAP from the LCP configure-request. The default value is Disable.

Using the BCC

The BCC does not allow you to configure this parameter.

Using Site Manager

To allow a remote peer to reject the use of PAP authentication for this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Allow PAP Reject**. (See page A-25.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Customizing CHAP

The Challenge Handshake Authentication Protocol imposes network security by requiring that the peers share a plain-text secret. You specify that secret, as well as other CHAP parameters, by configuring the parameters described in the next sections. If you have not enabled CHAP, ignore these parameters.

Note: For dial services that use CHAP, you must configure the CHAP secret and the CHAP local name through the Dial menu. See *Configuring Dial Services* for details.

Specifying the CHAP Secret

If you have enabled CHAP, specify the secret. There is no default value. The function of the CHAP secret is similar to a password, but its use is slightly different. Both peers on a link must have the same secret to correctly calculate responses to challenges either one of them may send to the other during the authentication process and network-layer negotiation phase. You can assign a text string up to 20 characters long as the CHAP secret for this interface.

Specifying the CHAP Local Name

A local CHAP name informs the peers of each other's identity. Specify the CHAP local name as a text string of up to 20 characters. There is no default value.

If you configure CHAP as an authentication protocol, you *must* use CHAP Local Name for router identification on a dial-on-demand, bandwidth-on-demand, or dial backup line. If you do not configure CHAP, you *cannot* use CHAP Local Name for identification; instead, you must configure PAP.

Specifying the CHAP Authentication Challenge Interval

The CHAP Periodic Timer parameter indicates the interval (in seconds) that must elapse between CHAP challenges. You can specify any number of seconds. Setting this value to 0 (the default) disables the timer. A reasonable value for this parameter is 60.

PPP allows repeated authentication challenges at an interval (in seconds) that either peer on the link can specify. The timer begins counting when an authentication phase has completed. A new challenge does not begin until the amount of time you specify elapses.

Enabling PAP Fallback

If the peer sends a configure-NAK packet, rejecting CHAP as the authentication protocol, and if you have enabled PAP fallback, the router offers PAP as the authentication protocol. You must also have enabled PAP and provided a PAP password.

Setting the Enable PAP Fallback parameter to Enable causes a fallback to PAP if you have selected CHAP as the authentication protocol, but the peer rejects CHAP. The default value is Disable. Set this parameter to Enable if you mix authentication types in the same pool.

Configuring PPP Interoperability with CLAM

If you configure a CHAP local name on a Bay Networks router that connects to a Corporate LAN Access Module (CLAM™) router, that local name is used to negotiate the link. If you do not configure a CHAP Local Name, Site Manager uses *BAYNETWORKS* as a default CHAP local name.

Using the BCC

The BCC does not allow you to configure these parameters.

Using Site Manager

To specify a CHAP secret, CHAP local name, CHAP authentication challenge interval, and enable PAP fallback for this interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **CHAP Secret**. (See page A-24.)	
5. Set **CHAP Local Name**. (See page A-24.)	
6. Set **CHAP Periodic Timer**. (See page A-25.)	
7. Set **Enable PAP Fallback**. (See page A-21.)	
8. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Setting Up Link Quality Monitoring

When you turn on the link quality monitoring and reporting function for an interface, PPP monitors the quality of the point-to-point link as a percentage of sent packets received on each end of the link. When the average quality falls below the threshold you specify, PPP brings down the link. The driver software automatically brings the link back up and renegotiates the connection.

By default, link quality monitoring is disabled. If you do not want to enable this feature, accept the default value.

Note: PPP supports link quality monitoring over standard synchronous interfaces only. PPP does not support link quality monitoring over asynchronous or high-speed serial interfaces (HSSI). BayStream software, however, does support both link quality monitoring and link quality reporting over HSSI interfaces.

If two routers are configured for different link quality reporting periods, they negotiate to the lower value, so that the period is the same on both sides of the link.

Enabling Link Quality Monitoring and Reporting

To turn on link quality monitoring and reporting for the interface, set the Link Quality Protocol parameter to LINKQR.

When you enable link quality monitoring and reporting through the link quality protocol, you are turning on monitoring only for the local router. The router on which you enable it is responsible for monitoring link quality for the connection. By default, link quality monitoring and reporting is disabled.

If you do not enable link quality monitoring and reporting, ignore the rest of the link quality parameters.

Establishing the Timing of Link Quality Reports

You can specify which peer is responsible for running the link quality report timer and set the maximum interval between the transmission of link quality report packets.

Designating the Link Quality Report Timekeeper

This parameter deals with the *remote* peer, not the local one. The setting determines whether the remote peer runs the link quality report (LQR) timer for the connection. Setting this parameter enables or disables the remote peer's LQR timer.

The peer whose timer is enabled generates one LQR packet for each interval specified in the LQR Reporting Period parameter. The peer whose timer is disabled verifies that the other peer did, in fact, send an LQR. If three successive LQRs are not received, the receiving peer disables the connection. Accept the default, Enable, if you want the remote peer router to maintain an LQR timer for the interface. Reset this parameter to Disable if you do not want the peer to maintain the LQR timer for the interface.

Specifying the Link Quality Reporting Period

The LQR Reporting Period parameter specifies the maximum number of seconds between the transmission of LQR packets. Enter a number representing the interval between the transmission of LQR packets. The value of this parameter can be from 1 through 120 seconds. The default value is 3 seconds.

Specifying the Inbound Link Quality

The Inbound Link Quality parameter specifies the minimum acceptable success rate (percentage) of packets the peer router transmits and this router receives on this interface over the last 5 LQR reporting periods. If the percentage drops below the inbound link quality you specify, the router brings down the link until the percentage increases to an acceptable level.

The default value for this parameter is 90 (percent). You can specify values in the range 1 through 100 (percent).

Specifying the Outbound Link Quality

The Outbound Link Quality parameter specifies the minimum acceptable success rate (percentage) of packets the router transmits and the peer router receives on this interface. If the percentage drops below the outbound link quality you specify, the router brings down the link until the percentage increases to an acceptable level.

The default value for this parameter is 90 (percent). You can specify values in the range 1 through 100 (percent).

Using the BCC

Note: A summary example, showing the use of all the BCC link monitoring commands, follows these syntax descriptions.

1. **Enable link quality monitoring.**

   Enabling link quality monitoring on the interface allows all the other link quality monitoring parameters to function. Navigate to the IP prompt and enter the following command.

   link-quality-protocol *value*

   value is

   none
   LINKQR

2. **Enable the peer LQR timer.**

   To specify whether the remote peer should maintain the LQR timer for the interface, enter the following command after setting the link quality protocol to LINKQR.

   peer-lqr-timer *value*

   value is

   enable
   disable

3. **Set the LQR reporting period.**

   To specify the LQR reporting period, enter the following command.

   lqr-reporting-period *seconds*

   seconds is an integer in the range 1 through 120.

4. **Set the inbound link quality.**

   To specify the inbound link quality, enter the following command after setting the link quality protocol to LINKQR.

   lqr-percentage-received *percent*

   percent is an integer in the range 0 through 100.

5. **Set the outbound link quality.**

   To specify the outbound link quality, enter the following command after setting the link quality protocol to LINKQR.

   lqr-percentage-sent *percent*

   percent is an integer in the range 0 through 100.

Summary Example for BCC Link Monitoring Commands

This example shows, for the PPP line on slot 3, circuit 1, how to use BCC to

- Enable link quality monitoring.
- Specify that the remote peer should maintain the LQR timer.
- Specify an LQR reporting period of 5 seconds.
- Set the acceptable inbound success rate to 85.
- Set the acceptable outbound success rate to 85.

```
line/3/1# link-quality-protocol LINKQR
line/3/1# peer-lqr-timer enable
line/3/1# lqr-reporting-period 5
line/3/1# lqr-percentage-received 85
line/3/1# lqr-percentage-sent 85
```

Using Site Manager

To configure link quality monitoring on this PPP interface, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Set **Link Quality Protocol**. (See page A-21.)	
4. Set **Peer Link Quality Report Timer**. (See page A-22.)	
5. Set **LQR Reporting Period**. (See page A-22.)	
6. Set **Inbound Link Quality**. (See page A-23.)	
7. Set **Outbound Link Quality**. (See page A-23.)	
8. If you have no other Interface parameters to configure, click on **OK**. Otherwise, continue with the Interface configuration.	The Configuration Manager window opens.

Specifying the Asynchronous Modem Control Character Map

During LCP negotiations, the peers negotiate the characters that they will recognize as asynchronous modem control characters. PPP creates a 32-bit map that represents the negotiated control characters. Both routers use this map in sending and receiving data packets. While the default value serves for almost all modems, you can configure the map for other modem control characters if necessary.

The async control character map specifies a value representing one or more asynchronous modem control characters for the peer to recognize (“escape”) and that may occur in the data packet. Each bit in the map corresponds to one control character, 0x00 (the right end of the map) through 0x1f (the left end of the map); that is, 0 through 31, decimal. The actual map is a value used essentially as a mask. For example, the default map value, 0xa0000 (655360 decimal) allows the escaping of the control characters 0x11 (XON) and 0x13 (XOFF) if they occur in the data stream. The values 0x7d and 0x7e are always escaped.

If you have a modem that requires control characters different from the default, you can build your own async control character map. Determine the corresponding bit for each character by converting the hex value of the control character to decimal. For example, 0x1f = 31 decimal; so to escape that character, set the leftmost bit in the map. Do the same thing for each control character. Once you’ve decided what bits in the map to set, you can enter either the hex character equivalent to the bit string or the decimal equivalent. To escape all control characters in the packet, set the map to 0xffffffff. For a description of how PPP encodes escaped control characters in the data stream, refer to Chapter 2.

PPP displays the decimal number equivalent to the string and uses that value in its link negotiations.

Using the BCC

The BCC does not allow you to configure this parameter.

Using Site Manager

To allow the peers to negotiate the use of asynchronous modem control characters for this line, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Set **Async Control Character Map**. (See page A-26.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Disabling Loopback Checking

For test purposes, you can disable the loopback test that the peer normally performs as part of its network integrity checking. The loopback test ensures that a peer is talking to the network, not to itself.

To disable loopback detection, set the Magic Num Disable parameter to Disable. After disabling this parameter, you must explicitly set it to Enable to re-enable loopback checking.

Using the BCC

Navigate to the line prompt for the circuit and enter

magic-number *value*

value is

enable
disable

For example, the following command disables loopback checking on the interface 3/1.

```
line/3/1# magic-number disable
```

Using Site Manager

To disable loopback checking for this line, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.
4. Set **Magic Num Disable**. (See page A-27.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Setting the Maximum Receive Unit (MRU)

In Version 12.00, the default Maximum Receive Unit (MRU) parameter value for PPP is 1500, for compatibility with RFC 1661. If you have a network with both Version 11.02 (or later) and pre-11.02 Bay Networks routers, or Corporate LAN Access Module (CLAM) routers configured with dial-on-demand, standby, or dial backup circuits, make sure that the value you set for the PPP MRU parameter is the same for the central-site router and the remote-site routers.

To accomplish this task, consider one of the following options:

- Upgrade all routers to Version 11.02 (or later) simultaneously.

  We strongly recommend this option.

- Upgrade the central-site router to Version 11.02 (or later), leaving the remote-site routers untouched. Then change the default MRU value on the central-site router to 1590 bytes.

- As you upgrade each remote-site router software to Version 11.02 (or later), set its MRU value to 1590, unless you can segregate the 11.02 (or later) remote sites into their own demand pool. You can do this if some of the remote-site routers are CLAM routers, provided they are running a CLAM release prior to 3.522R. CLAM routers running software earlier than 3.522R let you set the default MRU value to 1590.
- If some remote-site CLAM routers are running release 3.522R, then you cannot set the MRU value to 1590. In this case, isolate those CLAM routers in their own demand pool on the 11.02 (or later) router and set the MRU value of that pool to 1500.
- Upgrade the central-site router to Version 11.02 (or later), and set the default MRU value to 1500. Then reconfigure all remote-site routers dialing into that demand pool with the same MRU value.

  For pre-11.02 routers, change the MRU setting to 1500.
- Change the MRU value in the Sync Driver MTU attribute (the 1510 value becomes 1500 after subtracting CRC and PPP headers) of the pre-11.02 router to 1510. CLAM routers running Release 3.52R use the default setting of 1500.
- If you upgrade the central-site router to 11.02 (or later) and the default MRU value of 1500 is taken on one pool (to satisfy 3.522R CLAM routers or 11.02 [or later] routers), you can choose a different default value (for example, 1590) for a different pool that the 11.02 or pre-3.522R CLAM router dials into.

Using the BCC

The BCC does not allow you to configure this parameter.

Using Site Manager

To set the MRU for this line, do the tasks in the following table.

Site Manager Procedure	
You do this	**System responds**
1. From the Protocols menu, choose **PPP**.	The Interfaces menu appears.
2. Choose **Interfaces.**	The Interfaces window opens.
3. Choose **Lines**.	The Lines window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Set **MRU Size (bytes)**. (See page A-28.)	
5. If you have no other PPP line parameters to configure, click on **OK**. Otherwise, continue with the Lines configuration.	The Interfaces window opens.

Enabling RFC 1661 Compliance for Dial Circuits

To enable or disable RFC 1661 compliance on a dial circuit, do the tasks in the following table.

Site Manager Path	
You do this	**System responds**
1. In the Configuration Manager window, choose **Protocols.**	The Protocols menu opens.
2. Choose **PPP.**	The PPP menu opens.
3. Choose **Interfaces**.	The PPP Interface List window opens.
4. Click on **Lines**.	The PPP Line List window opens.
5. Set the **RFC1661 Compliance** parameter. (See page A-28.)	
6. Click on **Done**.	You return to the PPP Interface List window.
7. Click on **Done**.	You return to the Configuration Manager window.

Viewing Line Statistics for Multilink Circuits

To view the statistics that PPP collects for multilink circuits, use the Technician Interface software to access the PPP MIB. For instructions on how to use this software, refer to *Using Technician Interface Software.* Appendix C lists the PPP multilink statistics and describes the data that they record. The key statistics to check are the following:

- In the *wfPppCircuitEntry* MIB:
  - -- *wfPppCircuitMlFragPerm* indicates that fragmentation is enabled.
  - -- *wfPppCircuitMlFragTriggerSize* indicates the smallest-size packet that PPP may fragment.
  - -- *wfPppCircuitMaxBuffers* is the maximum allowable number of buffers for this circuit.
  - -- *wfPppCircuitMaxLinks* is the maximum number of links allowed in the multilink bundle for this circuit at any one time.
- In the *wfPppMlStatsEntry* MIB:
  - -- *wfPppMlStatsReSeqBufferCnt* is the current count of packets (not fragments) that the receiver has buffered because they arrived out of order. To analyze the effects of fragmentation, periodically observe this value under a typical traffic load *without* fragmentation enabled on the peer router, and then observe the value *with* fragmentation enabled on the peer router. Typically, this number is higher in configurations with greatly differing line speeds. This number should go down when fragmentation is enabled. If this number is constantly at or near the maximum number of buffers allowed, as indicated in *wfPppCircuitMaxBuffers*, reset the maximum number of buffers allowed to a higher number. In addition, the higher the value of *wfPppCircuitMaxLinks*s, the more likely it is you'll need to increase *wfPppCircuitMaxBuffers*.
  - -- *wfPppMlStatsReSeqBufferMax* is the maximum that *wfPppMlStatsReSeqBufferCnt* ever reached.
  - -- *wfPppMlStatsNumPktsFragmented* counts the number of packets that have been fragmented (transmit only). This indicates how often the router judges that fragmentation is necessary.

- -- *wfPppMlStatsTxPkts* counts the total number of packets transmitted by multilink. Comparing this to the number of packets fragmented (*wfPppMlStatsNumPktsFragmented*) helps you see how well the link is doing and whether you need to adjust parameters such as the minimum size of packets to be considered for fragmentation.
- -- *wfPppMlStatsReasmFails* is an event counter of failures to reassemble a fragmented packet. If this number is high, either you are losing fragments or your reassembly buffer count is at or near the maximum number of buffers allowed, as indicated in *wfPppCircuitMaxBuffers*. Reset the maximum number of buffers allowed to a higher number.
- -- *wfPppMlStatsReassmBufferCnt* is the number of fragments that the receiver has stored pending reassembly. Typically, this number is higher in configurations with greatly differing line speeds. If this number is constantly at or near the maximum number of buffers allowed, as indicated in *wfPppCircuitMaxBuffers*, reset the maximum number of buffers allowed to a higher number.
- -- *wfPppMlStatsReassmBufferMax* is the maximum number that *wfPppMlStatsReassmBufferCnt* ever reached.
- -- *wfPppMlStatsExceededBufferMax* indicates the number of times the sum of *wfPppMlStatsReassmBufferCnt* and *wfPppMlStatsReSeqBufferCnt* exceeded the specified maximum allowable number of buffers, as indicated in *wfPppCircuitMaxBuffers*. As a side effect of reaching or exceeding *wfPppMlStatsExceededBufferMax,* you may see the value of *wfPppMlStatsSeqNumberArrived Late* increase. If so, it may indicate that you should increase *wfPppCircuitMaxBuffers*.

- In the *wfSyncEntry* MIB:
  - -- *wfSyncRejectsRx* counts the number of times a packet arrives that is larger than a receive buffer. *wfSyncRejectsTx* counts the number of times a packet grows larger than its transmit buffer. If either of these conditions occurs, lower the size of the maximum transmission unit (MTU), *wfSyncMtu*, on both the local and remote peers.

Where to Go Next

Go to Chapter 1, “Starting PPP Services for instructions on how to start PPP on your router.

Go to Chapter 2, “PPP Concepts to learn more about PPP concepts and characteristics.

Go to Appendix A for a list of all PPP parameters.

Go to Appendix B for a list of PPP parameter default values.

Go to Appendix C for a list of the PPP statistics that you can view.

Go to Appendix D for descriptions of the BCC **show** commands for BCC.

Appendix A
PPP Parameters

This appendix lists the parameters for the PPP interfaces that you can configure on the router. For each PPP parameter, this appendix gives the Site Manager path, the default setting, all valid parameter options or ranges, the parameter function, instructions for setting the parameter, and the Management Information Base (MIB) object ID. Refer to Chapter 3 for a full description of the tasks to which these parameters pertain.

After you enable PPP, you can edit all PPP parameters. For instructions on using Site Manager to edit PPP parameters, refer to *Configuring and Managing Routers with Site Manager*, as appropriate for your platform. Alternatively, you can use the BCC, as described in Chapter 3, to edit certain PPP line parameters. You can also use Technician Interface **set** and **commit** commands to modify parameter values in the MIB object ID. This process is equivalent to modifying parameters using Site Manager.

Caution: The Technician Interface does not verify the validity of the parameter values that you enter. Entering an invalid value can corrupt your configuration.

The following sections deal with the parameters in two groups: those that pertain to configuring PPP on the interface and those that you use to configure PPP on individual lines on the interface. These correspond to Site Manager's PPP Interfaces and PPP Line Lists windows, respectively.

PPP Interface Parameter Descriptions

Use the following guidelines to configure the PPP Interface parameters. The order of presentation corresponds to the order of fields in the Site Manager PPP Interface Lists window, and also (approximately) to the order of items in the *wfPppCircuitEntry* MIB.

Figure A-1 shows the Site Manager PPP Interface Lists window.

Figure A-1. Site Manager PPP Interface Lists Window

Note: In BayStream software environments, only the IP Enable parameter is meaningful. In the BayStream environment, ignore all other PPP interface parameters.

Parameter: IP Enable

Path: Protocols > PPP > Interfaces

Default: If you enable IP support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol for IP.

This parameter does *not* enable or disable IP routing services for the interface; it affects the network control protocol for IP. However, disabling the network control protocol for IP stops IP traffic from being routed over this interface.

Instructions: To stop IP traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.12

Parameter: OSI Enable

Path: Protocols > PPP > Interfaces

Default: If you enable Open Systems Interconnect (OSI) support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable | Disable

Function: Enables or disables the network control protocol for OSI.

This parameter does *not* enable or disable OSI routing services for the interface; it affects the network control protocol for OSI. However, disabling the network control protocol for OSI stops OSI traffic from being routed over this interface.

Instructions: To stop OSI traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.13

Parameter: **XNS Enable**

Path: Protocols > PPP > Interfaces

Default: If you enable XNS support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for XNS.

This parameter does *not* enable or disable XNS routing services for the interface; it affects the network control protocol for XNS. However, disabling the network control protocol for XNS stops XNS traffic from being routed over this interface.

Instructions: To stop XNS traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.14

Parameter: **DECnet IV Enable**

Path: Protocols > PPP > Interfaces

Default: If you enable DECnet IV support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for DECnet IV.

This parameter does *not* enable or disable DECnet IV routing services for the interface; it affects the network control protocol for DECnet IV. However, disabling the network control protocol for DECnet IV stops DECnet IV traffic from being routed over this interface.

Instructions: To stop DECnet IV traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.15

Parameter: AppleTalk Enable

Path: Protocols > PPP > Interfaces

Default: If you enable AppleTalk support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for AppleTalk.

This parameter does *not* enable or disable AppleTalk routing services for the interface; it affects the network control protocol for AppleTalk. However, disabling the network control protocol for AppleTalk stops AppleTalk traffic from being routed over this interface.

Instructions: To stop AppleTalk traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.16

Parameter: IPX Enable

Path: Protocols > PPP > Interfaces

Default: If you enable Internet Packet Exchange (IPX) support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for IPX.

This parameter does *not* enable or disable IPX routing services for the interface; it affects the network control protocol for IPX. However, disabling the network control protocol for IPX stops IPX traffic from being routed over this interface.

Instructions: To stop IPX traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.17

Parameter: Bridge Enable

Path: Protocols > PPP > Interfaces

Default: If you enable the bridge when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for the bridge.

This parameter does *not* enable or disable bridging services for the interface; it affects the network control protocol for the bridge. However, disabling the network control protocol for the bridge stops traffic from being bridged over this interface.

Instructions: To stop traffic from being bridged over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.18

Parameter: VINES Enable

Path: Protocols > PPP > Interfaces

Default: If you enable VINES support when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for VINES.

This parameter does *not* enable or disable VINES routing services for the interface; it affects the network control protocol for VINES. However, disabling the network control protocol for VINES stops VINES traffic from being routed over this interface.

Instructions: To stop VINES traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.19

Parameter: CCP Enable

Path: Protocols > PPP > Interfaces

Default: If you enable data compression when you configure PPP on this interface, this parameter is automatically set to Enable. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables data compression.

This parameter does *not* enable or disable data compression for the interface. However, disabling the Compression Control Protocol (CCP) stops data compression over this interface.

Instructions: To stop compression over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.49

Parameter: IPV6 Enable

Path: Protocols > PPP > Interfaces

Default: If you enable Internet Protocol, version 6 (IPv6) support when you initially configure PPP on this interface, then the IPv6 parameter is enabled by default for PPP. Otherwise, the default is Disable.

Options: Enable │ Disable

Function: Enables or disables the network control protocol for IPv6.

This parameter does not enable or disable IPv6 routing services for the interface. However, disabling the network control protocol for IPv6 stops IPv6 traffic from being routed over this interface.

Instructions: To stop IPv6 traffic from being routed over this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.69

Parameter: Remote IP Address

Path: Protocols > PPP > Interfaces

Default: 0.0.0.0

Options: Any valid IP address

Function: Specifies the IP address the peer router should use. This interface includes this IP address in NCP negotiations.

Instructions: If you want to specify an IP address for the peer router, enter it here.

If this interface has been up and running, you must also set the IP Enable parameter to Disable, apply the change, and then reset the IP Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.22

Parameter: IPX Network Number

Path: Protocols > PPP > Interfaces

Default: None

Options: Any valid, unique, unreserved network number. This number must be a string of up to eight hexadecimal characters. (0xffffffff is invalid.)

Function: Specifies a network number used to negotiate the link. The negotiated number must be unique. It cannot be a previously assigned network number.

Instructions: Enter a valid IPX network number for this PPP interface.

The network number does not have to be the same on both sides of the link; PPP negotiates the higher of the two numbers. Note also that the negotiated IPX network number may be 0 on both sides of the link. In this case, IPX defines the link's network number.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.24

Parameter: IPX Remote Node Number

Path: Protocols > PPP > Interfaces

Default: None

Options: Any valid IPX node number

Function: Specifies the IPX node number the peer router should use. This interface includes this IPX remote node number in NCP negotiations.

Instructions: If you want to specify an IPX node number for the peer router, enter it here.

If this interface has been up and running, you must also set the IPX Enable parameter to Disable, apply the change, and then reset the IPX Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.26

Parameter: Remote AppleTalk Node

Path: Protocols > PPP > Interfaces

Default: None

Options: Any valid AppleTalk node number

Function: Specifies the AppleTalk node number the peer router should use. This interface includes this AppleTalk node number in NCP negotiations.

Instructions: If you want to specify an AppleTalk node number for the peer router, enter it here.

If this interface has been up and running, you must also set the AppleTalk Enable parameter to Disable, apply the change, and then reset the AppleTalk Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.36

Parameter:	**AppleTalk Routing Protocol**
Path:	Protocols > PPP > Interfaces
Default:	RTMP
Options:	RTMP (Routing Table Management Protocol)
Function:	Specifies the AppleTalk routing update protocol that this interface wants the peer router to use. This interface specifies AppleTalk RTMP as the routing update protocol in NCP negotiations.
Instructions:	Accept the default, RTMP.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.38

Parameter:	**Bridge Ethernet**
Path:	Protocols > PPP > Interfaces
Default:	Enable
Options:	Enable | Disable
Function:	Specifies whether this PPP interface accepts bridged traffic that is Ethernet encapsulated, then forwards it over the PPP network.
Instructions:	Set to Disable if you do not want the PPP interface to accept bridged, Ethernet-encapsulated frames. If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, apply the change, and then reset the Bridge Enable parameter to Enable to implement your changes.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.40

Parameter: Bridge FDDI

Path: Protocols > PPP > Interfaces

Default: Enable

Options: Enable | Disable

Function: Specifies whether this PPP interface accepts bridged traffic that is FDDI encapsulated, then forwards it over the PPP network.

Instructions: Set to Disable to refuse bridged, FDDI-encapsulated frames on this PPP interface.

If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, apply the change, and then reset the Bridge Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.42

Parameter: Bridge Token Ring

Path: Protocols > PPP > Interfaces

Default: Enable

Options: Enable | Disable

Function: Specifies whether this PPP interface accepts bridged traffic that is token ring encapsulated, then forwards it over the PPP network. The token ring network must support source routing; the router expects all token ring-bridged frames to be source routed.

Instructions: Set to Disable if you do not want the PPP interface to accept bridged, token ring-encapsulated frames.

If this interface has been up and running, you must also set the Bridge Enable parameter to Disable, apply the change, and then reset the Bridge Enable parameter to Enable to implement your changes.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.44

Parameter: PPP Mode

Path: Protocols > PPP > Interfaces

Default: Multilink for a dial-on-demand or bandwidth-on-demand circuit

Normal for a nonmultilink circuit

Options: Normal for a nonmultilink circuit

Multilink | Monitor for a dial-on-demand or bandwidth-on-demand circuit

Normal | Multilink for all other circuit types

Function: Specifies the type of multiline or multilink connection on this interface.

Instructions: The set of available options depends on the type of circuit you're configuring. Select one of the following values:

Normal - to configure a nonmultilink circuit

Multilink - to enable the multilink feature

Monitor - to designate the local router as the multilink monitor

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.50

Parameter: Multilink Fragmentation

Path: Protocols > PPP > Interfaces

Default: Permitted

Options: Permitted | Prohibited

Function: This parameter is active only for multilink. Allows packet fragmentation on multilink circuits, when needed.

Instructions: Accept the default, Permitted, if you want to allow multilink packet fragmentation. Otherwise, specify Prohibited.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.2.1.51

Parameter:	**Fragmentation Trigger Size**
Path:	Protocols > PPP > Interfaces
Default:	256 (bytes)
Range:	64 through the maximum transmission unit for the circuit
Function:	This parameter is active only for multilink. Specifies the minimum size of a packet that multilink will fragment.
Instructions:	When packet fragmentation over multilink is permitted, accept the default or specify the minimum packet size that PPP will consider fragmenting.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.2.1.57

PPP Line Parameter Descriptions

Use the following guidelines to configure the PPP Lines parameters. The order of presentation corresponds to the order of fields in the PPP Line Lists window, and also (approximately) to the order of items in the *wfPppLineEntry* MIB. Figure A-2 shows the Site Manager PPP Line Lists window. In the path names that follow, bold text indicates that in Site Manager, you invoke the PPP Line Lists window by clicking on the **Lines** button on the PPP Interface Lists window.

Figure A-2. Site Manager PPP Line Lists Window

Parameter: Enable (LCP)

Path: Protocols > PPP > Interfaces > **Lines**

Default: Enable

Options: Enable | Disable

Function: Enables or disables the Link Control Protocol (LCP) on the PPP interface. Disabling this parameter generates a “close” event to LCP. Similarly, enabling this parameter generates an “open” event to LCP.

Disabling, then re-enabling this parameter forces the interface to renegotiate the link.

Instructions: To disable LCP on this interface, set this parameter to Disable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.2

Parameter: **Restart Timer in Seconds**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 3 (seconds)

Range: 1 through 1000

Function: Specifies the number of seconds that the restart timer waits before retransmitting data.

Instructions: Accept the default value of 3.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.7

Parameter: **Seconds between Xmit of Echo-Request**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 0 (seconds)

Range: 0 through 100

Function: Specifies the number of seconds that the router waits between the transmission of echo-request packets. A value of 0 means that this parameter is turned off.

Instructions: Accept the default value of 0 or enter an integer value in the range 0 through 100.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.8

Parameter: **Echo-Reply Acceptable Loss**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 3 (packets)

Range: 1 through 100

Function: Specifies the maximum number of unacknowledged echo-reply packets that the router will transmit before declaring the point-to-point link down.

Instructions: Accept the default value of 3.

If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.9

Parameter: **Max Configure-Requests**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 10 (packets)

Range: 1 through 100000

Function: Specifies the maximum number of unacknowledged configure-request packets that the router will transmit before assuming that the peer router on the other end of the link is unable to respond. The link is then brought down. Valid acknowledgments include configure-ACK, configure-NAK, or configure-reject packets.

Instructions: Accept the default value of 10.
If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.10

Parameter: **Max Terminate-Requests**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 2 (packets)

Range: 1 through 100

Function: Specifies the maximum number of unacknowledged terminate-request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond. The valid acknowledgment is a terminate-ACK packet.

Instructions: Accept the default value of 2.

If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.11

Parameter:	**Max Configuration Failure Count**
Path:	Protocols > PPP > Interfaces > **Lines**
Default:	10
Range:	1 through 100
Function:	Specifies the maximum number of configure-NAK packets the router sends before sending a configure-reject packet for those options that it does not agree with.
Instructions:	Accept the default value of 10. If you enter a different value, you must set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable to implement your change.
MIB Object ID:	1.3.6.1.4.1.18.3.5.9.2.1.1.12

Parameter: Local Authentication Protocol

Path: Protocols > PPP > Interfaces > **Lines**

Default: CHAP for dial services
None for all others

Options: None | PAPAUTH | CHAP

Function: Specifies the type of authentication protocol that this interface uses: none, PAP (Password Authentication Protocol), or CHAP (Challenge Handshake Authentication Protocol).

Instructions: If you do not want to enable security features on this interface, accept the default, None.

To enable Password Authentication Protocol, select PAPAUTH. Then do the following:

- Define the Local PAP ID and Local PAP Password parameters for this interface.
- Set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

To enable Challenge Handshake Authentication Protocol, select CHAP. Then do the following:

- Define the CHAP Secret, CHAP Local Name, and CHAP Periodic Timer parameters for this interface. Find these parameters by scrolling further through the list of line parameters.
- Set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For all dial services, you must use PAP or CHAP, either of which provides an identification mechanism that is essential to bring up demand, backup, and bandwidth lines. You must configure CHAP Local Name, CHAP Secret, PAP ID, and PAP Password through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.15

Parameter: Local PAP ID

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP ID assigned to this interface. During the interface's authentication phase, all password authenticate-request messages the peer router sends to this interface must include the correct PAP ID. Otherwise, the interface sends an authenticate-NAK message and the link is not created.

Instructions: If you have not enabled PAP, ignore this field.

If you set the Local Authentication Protocol parameter to PAPAUTH, specify a unique local PAP ID for this interface. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For dial services that use PAP, you must configure the local PAP ID through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.17

Parameter: Local PAP Password

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP password assigned to this interface. During the interface's authentication phase, all password authenticate-request messages sent to this interface by the peer router must include the correct PAP password. Otherwise, the peer router sends an authenticate-NAK message and the link is not created.

Instructions: If you have not enabled PAP, ignore this field.

If you set the Local Authentication Protocol to PAPAUTH, specify a unique local PAP password for this interface. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For dial services that use PAP, you must configure the local PAP password through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.18

Parameter: Remote PAP ID

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP ID assigned to the remote peer router. During the interface's authentication phase, this interface must include the correct remote PAP ID in all password authenticate-request messages it sends to the peer router, or the peer router sends an authenticate-NAK message and the link is not created.

Instructions: If the remote peer does not have PAP enabled, ignore this field.

If the remote peer has PAP enabled, specify the remote PAP ID that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For dial services that use PAP, you must configure the remote PAP ID through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.19

Parameter: Remote PAP Password

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 25 characters

Function: Specifies the PAP password assigned to the remote peer router. During the interface's authentication phase, this interface must include the correct remote PAP password in all password authenticate-request messages it sends to the peer router. Otherwise, the peer router sends an authenticate-NAK message and the link is not created.

Instructions: If the remote peer has PAP enabled, specify the remote PAP password that identifies the remote peer. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For all dial services, you must configure the remote PAP password through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.20

Parameter: Enable PAP Fallback

Path: Protocols > PPP > Interfaces > **Lines**

Default: Disable

Options: Enable | Disable

Function: Enabling this parameter causes a fallback to PAP if you have selected CHAP as the authentication protocol, and an attempt to negotiate CHAP fails.

Instructions: Select Enable or Disable. Set this parameter to Enable if you mix authentication types in a pool. Remember that you must use an authentication protocol if you are using dial-on-demand, bandwidth-on-demand, or dial backup.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.32

Parameter: Link Quality Protocol

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: None | LINKQR

Function: Enables or disables the Link Quality Protocol for this interface.

Instructions: To enable link quality reporting, set this parameter to LINKQR. When you enable link quality reporting on one side of the connection, the router on which you enable it is responsible for monitoring link quality for the connection. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.21

Parameter: **Peer Link Quality Report Timer**

Path: Protocols > PPP > Interfaces > **Lines**

Default: Enable

Options: Enable | Disable

Function: This parameter deals with the *remote* peer, not the local one. The setting determines whether the remote peer runs the link quality report (LQR) timer for the connection. Setting this parameter enables or disables the remote peer's LQR timer.

The peer whose timer is enabled generates one LQR packet for each interval specified in the LQR Reporting Period parameter. The peer whose timer is disabled verifies that the other peer did, in fact, send an LQR. If the receiving peer does not receive three successive LQRs, it disables the connection.

Instructions: Use this parameter only when you have set the Link Quality Protocol parameter to LINKQR.

Accept the default, Enable, if you want the peer router to maintain an LQR timer for the interface. Reset this parameter to Disable if you do not want the peer to maintain the LQR timer for the interface. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.22

Parameter: **LQR Reporting Period**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 3 (seconds)

Range: 1 through 120

Function: Specifies the maximum number of seconds between the transmission of LQR packets.

Instructions: Use this parameter only when you set the Link Quality Protocol parameter to LINKQR.

Enter a number representing the interval between the transmission of LQR packets. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.23

Parameter: Inbound Link Quality

Path: Protocols > PPP > Interfaces > **Lines**

Default: 90 (percent)

Range: 0 through 100

Function: Specifies the minimum acceptable success rate (percentage) of packets the peer router transmits and this router receives on this interface over the last 5 LQR reporting periods. Use this parameter only when you enable the Link Quality Protocol parameter.

Instructions: If the percentage drops below the inbound link quality you specify, the router brings down the link until the percentage increases to an acceptable level.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.25

Parameter: Outbound Link Quality

Path: Protocols > PPP > Interfaces > **Lines**

Default: 90 (percent)

Range: 0 through 100

Function: Specifies the minimum acceptable success rate (percentage) of packets the router transmits and the peer router receives on this interface. Use this parameter only when you enable the Link Quality Protocol parameter.

Instructions: If the percentage drops below the outbound link quality you specify, the router brings down the link until the percentage increases to an acceptable level.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.27

Parameter: CHAP Secret

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 20 characters

Function: Specifies the CHAP secret you assign to this interface. The CHAP secret must be the same on both sides of the link. Both routers on a link must have the same secret to correctly calculate responses to challenges either one of them may send to the other during the authentication process and the network layer negotiation phase.

Instructions: If you have not enabled CHAP, ignore this field.

If you have enabled CHAP, specify the secret. To implement your changes, set the Enable (LCP) parameter to Disable, apply the change, and then reset the parameter to Enable.

For all dial services, you must configure CHAP Secret through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.31

Parameter: CHAP Local Name

Path: Protocols > PPP > Interfaces > **Lines**

Default: None

Options: Any text string; maximum 20 characters

Function: A local CHAP name informs the peers of each other's identity.

Instructions: If you configure CHAP as an authentication protocol, you *must* use CHAP Local Name for router identification on a bandwidth-on-demand, dial-on-demand, or dial backup line. If you do not configure CHAP, you *cannot* use CHAP Local Name for identification; instead, you must configure PAP.

For all dial services, you must configure CHAP Local Name through the Dial menu. See *Configuring Dial Services* for details.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.33

Parameter: CHAP Periodic Timer

Path: Protocols > PPP > Interfaces > **Lines**

Default: 0 (disabled)

Options: Any number of seconds. Setting this value to 0 disables the timer. A reasonable value for this parameter is 60.

Function: Allows for repeated authentication challenges at an interval (in seconds) that either peer on the link can specify. The timer begins counting when an authentication phase has completed. A new challenge does not begin until the amount of time you specify elapses.

Instructions: Accept the default or set this parameter to 60.

If you have not configured CHAP, ignore this field.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.35

Parameter: Allow PAP Reject

Path: Protocols > PPP > Interfaces > **Lines**

Default: Disable

Options: Enable | Disable

Function: Some peers do not use PAP. If you set this parameter to Enable, your router accepts the reject message from such a peer and removes PAP from the LCP configure-request.

Instructions: Select Enable or Disable.

If you have not configured PAP, ignore this field.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.39

Parameter: **Async Control Character Map**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 655360

Range: 0 through 4294967295 (0x00 through 0xFFFFFFFF)

Function: This parameter is relevant only if you use an asynchronous modem. During LCP negotiations, the peers negotiate the characters that they will recognize as modem control characters.

The async control character map specifies a value representing one or more asynchronous modem control characters for the peer to recognize ("escape") and that may occur in the data packet. Each bit in the map represents a control character from 0x00 through 0x1F. The default value serves for almost all modems. It escapes the asynchronous modem control sequence XON/XOFF (0x11 and 0x13) if they occur in the data stream. The values 0x7D and 0x7E are always escaped.

PPP displays the decimal number equivalent to the string and uses that value in its link negotiations.

Instructions: Accept the default value 655360 (0x000A0000) or enter the value corresponding to the asynchronous control character map for the character(s) that you want recognized ("escaped") in the data stream. It is unusual to require a value other than the default.

If you must create a different map, here's how to do it. The map consists of 32 bits. Each bit corresponds to one control character, 0x00 (the right end of the map) through 0x1F (the left end of the map); that is, 0 through 31, decimal.

If you have a modem that requires control characters different from the default, determine the corresponding bit for each character by converting the hex value of the control character to decimal. For example, 0x1F = 31 decimal, so to escape that character, set the leftmost bit in the map. Do the same thing for each control character to be escaped. Once you've decided what bits in the map to set, enter either the hex character equivalent to the bit string or the decimal equivalent. To escape all control characters in a packet, set the map to 0xFFFFFFFF.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.41

Parameter: **Authentication Timer**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 10

Range: 1 through 1000 (seconds)

Function: Sets the time limit the router waits for a response to its authentication messages.

Instructions: Accept the default value, 10 (seconds), or enter an integer in the range 1 through 1000. If you have not configured PAP or CHAP, ignore this field.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.43

Parameter: **Convergence Timer**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 300 (seconds)

Range: 1 through 5000 (seconds)

Function: Limits the amount of time PPP attempts to negotiate a dial-up connection. If the timer expires, the connection is dropped. This parameter is valid only for switched PPP interfaces.

Instructions: Accept the default value, 10 (seconds), or enter an integer in the range 1 through 1000.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.44

Parameter: **Magic Num Disable**

Path: Protocols > PPP > Interfaces > **Lines**

Default: Enable

Options: Enable | Disable

Function: Disables the loopback test that the peer normally performs as part of its network integrity checking. The loopback test ensures that a peer is talking to the network, not to itself.

Instructions: Accept the default value, Enable, unless you are testing the connection. After disabling this parameter, you must explicitly set it to Enable to reenable loopback checking.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.45

Parameter: **MRU Size (bytes)**

Path: Protocols > PPP > Interfaces > **Lines**

Default: 1500

Options: 1 to 4600

Function: Sets the maximum receive unit (MRU) size being used on the line.

Instructions: Accept the default value, 1500 bytes, or enter in the range 1 to 4600 bytes. If you have a network with Version 11.02 or Version 12.00 routers and also with earlier Bay Networks routers or Corporate Lan Access Module (CLAM) routers configured with dial-on-demand, standby, dial backup, or bandwidth on demand circuits, make sure that the value you set for the PPP MRU Size parameter is the same for the central-site and remote-site routers.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.48

Parameter: **RFC1661 Compliance**

Path: Protocols > PPP > Interfaces > **Lines**

Default: Disable

Options: Enable | Disable

Function: Enables RFC 1661 compliance for a PPP dial circuit.

Instructions: Select Enable to make the PPP dial circuit RFC 1661-compliant. Otherwise, accept the default.

MIB Object ID: 1.3.6.1.4.1.18.3.5.9.2.1.1.49

Appendix B
Default PPP Configuration

The PPP default configuration depends on which protocols you enable for the interface. Table B-1 and Table B-2 list the default PPP parameter settings.

Table B-1. PPP Interface Parameters

Parameter	Default
IP Enable OSI Enable XNS Enable DECnet IV Enable AppleTalk Enable IPX Enable Bridge Enable VINES Enable	Enabling support for any of these protocols when you configure PPP on this interface automatically sets the protocol's corresponding Enable parameter to Enable. Otherwise, the default is Disable.
CCP Enable	If you enabled data compression on this interface, Site Manager automatically sets this parameter to Enable. Otherwise, the default is Disable.
Remote IP Address	0.0.0.0
IPX Network Number	None
IPX Remote Node Number	None
Remote AppleTalk Node	None
AppleTalk Routing Protocol	RTMP
Bridge Ethernet	Enable
Bridge FDDI	Enable
Bridge Token Ring	Enable

(continued)

Table B-1. PPP Interface Parameters *(continued)*

Parameter	Default
PPP Mode	Normal for a nonmultilink circuit Multilink for a multilink circuit
Multilink Fragmentation	Permitted
Fragmentation Trigger Size	256

Table B-2. PPP Line Parameters

Parameter	Default
Enable (LCP)	Enable
Restart Timer in Seconds	3
Seconds between Xmit of Echo-Request	0
Echo-Reply Acceptable Loss	3
Max Configure-Requests	10
Max Terminate-Requests	2
Max Configuration Failure Count	10
Local Authentication Protocol	CHAP for dial services None for all others
Local PAP ID	None
Local PAP Password	None
Remote PAP ID	None
Remote PAP Password	None
Enable PAP Fallback	Disable
Link Quality Protocol	None
Peer Link Quality Report Timer	Enable

(continued)

Table B-2. PPP Line Parameters *(continued)*

Parameter	Default
LQR Reporting Period	3
Inbound Link Quality	90
Outbound Link Quality	90
CHAP Secret	None
CHAP Local Name	None
CHAP Periodic Timer	None
Allow PAP Reject	Disable
Async Control Character Map	655360 (0x000A000)
Authentication Timer	10
Convergence Timer	300
Magic Num Disable	Enable
MRU Size (bytes)	1500
RFC1661 Compliance	Disable

Appendix C
PPP Statistics

Table C-1 summarizes the PPP statistics you can view from the Site Manager Statistics Manager tool or from the Technician Interface.

Table C-1. PPP Statistics

MIB Object Name	What It Tells You
wfPppMlStatsCircuitID	Circuit number for this instance
wfPppMlStatsHomeSlot	Slot on which this multilink control subsystem exists
wfPppMlStatsLineCnt	Current count of lines in the multilink bundle
wfPppMlStatsBundleSpd	Current total bandwidth of the multilink bundle
wfPppMlStatsTxOctets	Number of octets transmitted by multilink
wfPppMlStatsTxPkts	Number of packets transmitted by multilink
wfPppMlStatsAvgTxListLen	Average number of packets received in the transient list by the Multilink Transmit gate
wfPppMlStatsRxOctets	Number of octets received without error
wfPppMlStatsRxPkts	Number of packets received by multilink
wfPppMlStatsReasmFails	Number of packet reassembly failures
wfPppMlStatsSeqNumberLost	Number of multilink packets considered to be lost on the wire
wfPppMlStatsSeqNumberArrivedLate	Number of multilink packets that arrive containing an old sequence number; that is, packets with a more current sequence number have already been sent up to NCP

(continued)

Table C-1. PPP Statistics *(continued)*

MIB Object Name	What It Tells You
wfPppMlStatsReSeqBufferCnt	Number of multilink packets currently stored in the ReSequencing buffer pool
wfPppMlStatsReSeqBufferMax	The maximum number of multilink packets stored in the ReSequencing buffer pool
wfPppMlStatsExceededBufferMax	The number of times a buffer needed to be stored by the Multilink Receive logic when the count of buffers stored, wfPppMlStatsReSeqBufferMax, was equal to the maximum allowable for this circuit,wfPppCircuitMaxBuffers
wfPppMlStatsLinkIdleEvents	The number of times the Multilink Receive logic detected a stored buffer received on a line what has been declared idle
wfPppMlStatsCalcPercent	Enable/disable calculating the percentage of multilink octets received on the line
wfPppMlStatsReassmBufferCnt	The number of multilink packets currently stored in the Reassembling buffer pools
wfPppMlStatsReassmBufferMax	The maximum number of multilink packets stored in the Reassembling buffer pools
wfPppMlStatsNumPktsFragmented	The number of multilink packets that were fragmented

Appendix D
Monitoring PPP Using the BCC show Command

This appendix describes how to use the BCC **show** command to obtain PPP statistical data from the management information base (MIB). The type and amount of data displayed depends on the specific PPP settings you want to view.

This appendix includes descriptions of the following **show** commands:

Command	Page
show ppp alerts	D-2
show ppp bad-packets	D-2
show ppp disabled	D-2
show ppp enabled	D-3
show ppp interfaces	D-3
show ppp ip	D-4
show ppp ipx	D-4
show ppp line	D-6
show ppp lqr	D-8

show ppp alerts

The BCC **show ppp alerts** command displays information about PPP exception conditions.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Module>/Conn	Names the physical interface.
Line State	The operational state of this line.
Protocol	The currently active protocol on this circuit.
State	Indicates whether PPP is enabled or disabled on this circuit.

show ppp bad-packets

The BCC **show ppp bad-packets** command displays information about invalid packets received on the specified circuit.

The output contains the following information:

Circuit Name	The circuit for which this command displays information.
# Bad Packets	Number of invalid packets received.
Last Bad Packet	Information about the last invalid packet received.

show ppp disabled

The BCC **show ppp disabled** command displays information about the protocols disabled on the specified PPP circuit.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Line #	The line within the circuit to which this information applies.
Protocol	The protocol disabled on this line.
State	The operational state of this line.

show ppp enabled

The BCC **show ppp enabled** command displays information about the protocols enabled on the specified PPP circuit.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Line #	The line within the circuit to which this information applies.
Protocol	The protocol enabled on this line.
State	The operational state of this line.

show ppp interfaces

The BCC **show ppp interfaces** command displays configuration information for each type of interface configured on each circuit.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Module>/Conn	Names the physical interface.
Driver State	The operational state of the driver, if one is present.
Protocol	The protocol or protocols configured on this circuit.
State	The operational state of each configured protocol.
Line State	The operational state of each line in the circuit.

show ppp ip

The BCC **show ppp ip** command displays information about the PPP IP configuration.

The output contains the following information:

Circuit	The circuit for which this command displays information.
State	The operational state of the interface.
Local Config	The IP address that this router wants to use.
Local Address	The IP address that the peer router wants the local router to use.
Remote Config	The IP address that this router wants the remote peer to use.
Remote Address	The IP address that the remote peer wants to use.

show ppp ipx

The BCC **show ppp ipx** command displays information about the PPP IPX configuration.

show ppp ipx config

The **show ppp ipx config** command displays summary information about the PPP IPX configuration.

The output contains the following information:

Circuit	The circuit for which this command displays information.
State	The operational state of the interface.
Network Number	The configured IPX network number.
Remote Node	The node number that the local router tells the remote peer to use if the peer sends a node number of 0.
Routing Protocol	The IPX routing protocol on the interface.

show ppp ipx name-local

The **show ppp ipx name-local** command displays information about the PPP IPX local router.

The output contains the following information:

Circuit name	Names the physical interface.
State	The operational state of the interface.
Local Router Name	The name of the local router.

show ppp ipx name-remote

The **show ppp ipx name-remote** command displays information about the PPP IPX remote peer router.

The output contains the following information:

Circuit name	Names the physical interface.
State	The operational state of the interface.
Remote Router Name	The name of the remote router.

show ppp ipx negotiated

The **show ppp ipx negotiated** command displays information about the PPP IPX negotiated connection.

The output contains the following information:

Circuit	Names the physical interface.
State	The operational state of the interface.
Network Number	The negotiated IPX network number.
Config Complete	Indicates whether IPXCP converged on all required options.
Routing Protocol	The negotiated IPX routing protocol used on the link.

show ppp line

The BCC **show ppp line** command displays information about the PPP lines configured for the specified interface.

show ppp line async-map

The **show ppp line async-map** command displays information about the PPP async control character map configured for the specified interface.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Module>/Conn	Names the physical interface.
Configured Async Map	The configured value of the async control character map.
Actual Async Map	The actual value of the async control character map.

show ppp line config

The **show ppp line config** command displays information about the configured PPP line parameter values for the specified interface.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Mod>/Conn	Names the physical interface.
LCP	The operational state of the Link Control Protocol.
Restart Timer	The number of seconds that the restart timer waits before retransmitting data.
Echo Req Freq	The number of seconds that the router waits between the transmission of echo-request packets.
Echo Rep Loss	The maximum number of unacknowledged echo-reply packets that the router transmits before declaring the point-to-point link down.
Max Conf Req	The maximum number of unacknowledged configure-request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond.
Max Term Req	The maximum number of unacknowledged terminate-request packets that the router transmits before assuming that the peer router on the other end of the link is unable to respond.
Max Conf Fail	The maximum number of configure-NAK packets that the router transmits before sending a configure-reject packet for those options that it does not agree with.

show ppp line params

The **show ppp line params** command displays information about the PPP line parameters configured for the specified interface.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Mod>/Conn	Names the physical interface.
LCP	The operational state of the Link Control Protocol.
Magic Number	The operational state of the loopback test that the peer normally performs as part of its network integrity checking.

MRU	The maximum receive unit size.
Local Auth. Prot	The type of authentication protocol that this interface uses.
Remote Auth. Prot.	The type of authentication protocol that the remote peer uses.

show ppp lqr

The BCC **show ppp lqr** command displays information about the configured PPP link quality values for the specified interface.

show ppp lqr config

The **show ppp lqr config** command displays information about the PPP link quality reporting configured for the specified interface.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Module>/Conn	Names the physical interface.
LQ Protocol	The Link Quality Protocol used on this interface.
Remote Timer	Specifies whether the remote peer runs the link quality report timer.
LQR Repeat Period	The maximum number of seconds between the transmission of LQR packets.
Inbound Quality	The minimum acceptable success rate (percentage) of packets that the peer router sent and this router received on this interface over the last five LQR reporting periods.
Outbound Quality	The minimum acceptable success rate (percentage) of packets that this router sent on this interface and the peer router received.

show ppp lqr stats

The **show ppp lqr stats** command displays information about the PPP link quality reporting statistics for the specified interface.

The output contains the following information:

Circuit	The circuit for which this command displays information.
Slot/<Mod>/Conn	Names the physical interface.
LCP State	The operational state of the Link Control Protocol.
LQR Repeat Period	The maximum number of seconds between the transmission of LQR packets.
Inbound Quality	The minimum acceptable success rate (percentage) of packets that the peer router sent and this router received on this interface over the last five LQR reporting periods.
Outbound Quality	The minimum acceptable success rate (percentage) of packets that this router sent on this interface and the peer router received.
LQR In	The current inbound quality.
LQR Out	The current outbound quality.

Index

A

acronyms, xviii

adding interfaces, 1-3

address
  IP, remote peer, 3-4

AFN, 2-13

allow PAP reject, 3-29

Allow PAP Reject parameter, A-25

AN, 2-13, 2-23

AppleTalk, 2-4
  configuring on a PPP interface, 3-6
  node number for remote peer, 3-6
  routing protocol, 3-6

AppleTalk Control Protocol, 2-4

AppleTalk Enable parameter, A-5, B-1

AppleTalk Routing Protocol parameter, A-10, B-1

ASN, 2-13, 2-23

async control character map, 2-24

Async Control Character Map parameter, A-26, B-3

asynchronous
  connection, 2-23
  modem, 2-23
  modem control characters, 2-23, 3-36

authentication, 3-24
  CHAP challenge interval, 3-30
  one-way, 2-9
  timer, 3-26

authentication protocols
  CHAP, 2-3, 2-8
  local, 3-24
  PAP, 2-3, 2-8
  setting parameters, A-18, A-24
  use with dial services, 2-8

Authentication Timer parameter, A-27, B-3

B

balancing traffic loads, 2-15

bandwidth-on-demand, 2-11, 2-15
  with multilink, 2-13

BayStream software, 2-12
  and LQM, 3-32
  HSSI link quality monitoring, 2-20
  IP Enable parameter, A-2

BCC show ppp command, D-1

BCC, starting, 1-3

BCC-configurable line parameters, 3-14

BCN, 2-13, 2-23

BLN, 2-13

BN, 2-23

BNCP, 2-4

BOFL synchronous line parameter, 2-24

Bridge Enable parameter, A-6, B-1

Bridge Ethernet parameter, A-10, B-1

Bridge FDDI parameter, A-11, B-1

Bridge Network Control Protocol, 2-4

Bridge Token Ring parameter, A-11, B-1

bridging
  enabling on a PPP interface, 3-7

buffer, 2-16

bundle, multilink, 2-14

C

CCP, 3-9

CCP Enable parameter, A-7, B-1

Challenge Handshake Authentication Protocol (CHAP), 2-3, 2-8, 2-11, 3-24
customizing, 3-29
setting parameters, A-18, A-24
use with dial services, 3-29
CHAP Local Name
identification mechanism, 2-11
CHAP parameters
Allow PAP Reject, A-25, B-3
CHAP Local Name, 3-30, A-24, B-3
CHAP Periodic Timer, 3-30, A-25, B-3
CHAP Secret, 3-30, A-24, B-3
circuit
initializing, 2-5
statistics, calculating and viewing, 3-42
CLAM router, 3-31
CLAM router, MRU size, A-28
CN, 2-13
code-reject packet, 2-5
comparing multiline and PPP multilink, 2-18
compatibility
previous versions, 2-15
compression
data, 2-22, 3-9, A-7
compression control protocol (CCP), 3-9, A-7
concepts, PPP, 2-1
configuration failure count, 3-22
configuration tools, starting, 1-3
configure-ACK packet, 2-5, 2-6
configure-NAK packet, 2-5, 2-6, 3-22
setting maximum number, A-17
configure-reject packet, 2-5, 2-6, 3-22
configure-request packet, 2-5
maximum number, 3-20
setting maximum number, A-16
configuring
multilink, 2-15
congestion monitor, 2-13, 2-15
conventions, text, xvi
convergence timer, 3-23
Convergence Timer parameter, A-27, B-3
Corporate LAN Access Module (CLAM) router, 3-31
Corporate LAN Access Module (CLAM) router, MRU size, A-28

D

data, A-7
data compression, 2-22, 3-9, A-7
data encryption, 3-13
data link control protocol, 2-2, 2-3
authentication, 2-8
data link layer, 2-2
data path,WAN, 2-12
datagram encapsulation, 2-2, 2-10
DECnet IV Enable parameter, A-4, B-1
DECnet IV support, enabling, 3-9
DECnet Phase IV Control Protocol, 2-4
defaults
interface parameters, B-1
deleting PPP, 1-6
device configuration, adding or modifying, 1-3
dial backup, 2-11, A-24
dial services, 2-11
bandwidth-on-demand, 2-11
dial backup, 2-11
dial-on-demand, 2-11
identification mechanism, 2-8
PPP support, 2-10
dial-on-demand, 2-11, A-24
implementation notes, 2-17
dial-up line
PPP support, 2-10
See also dial services
differences between multiline and multilink, 2-17
disabling loopback detection, 3-38, A-27
disabling PPP, 1-5
DSO, 2-13

E

Echo-Reply Acceptable Loss parameter, A-15, B-2
echo-reply packet, 2-5
  acceptable loss, 3-19
echo-request packet, 2-5, 2-22
  setting interval, 3-19
educational services, xx
Enable (LCP) parameter, A-14, B-2
Enable PAP Fallback parameter, A-21
encapsulation, 2-10
  datagram, 2-2
  frame structure, 2-10
Encrypt Enable encryption parameter, 3-13
encryption parameters, 3-13
endpoint discriminator, 2-3
escape characters, 2-23
establishing the PPP link, 2-5

F

fragmentation
  minimum size, 2-16
  packet, 2-16
Fragmentation Trigger Size parameter, A-13, B-2
frame structure, 2-10

H

high-speed serial interface (HSSI), 2-20, 3-32

I

inbound link quality, 2-20, 3-33
Inbound Link Quality parameter, A-23, B-3
initializing a PPP interface, 2-5
  (figure), 2-7
interface
  initializing, 2-5
  initializing with PPP (figure), 2-7
  unnumbered, 3-4
Interfaces window, A-13
interfaces, adding or modifying, 1-3
Internet Packet Exchange, 2-4
Internet Protocol (IP), 2-4
interoperability
  one-way authentication, 2-9
IP, 2-4
  enabling on a PPP interface, 2-25
IP address, remote peer, 3-4
IP Enable parameter, A-3, B-1
IPV6 Enable parameter, A-7
IPX, 2-4
  negotiated network number, 3-5
  network number for remote peer, 3-5
  node number for remote peer, 3-5
IPX Enable parameter, A-5, B-1
IPX Network Number parameter, A-8, B-1
IPX Remote Node Number parameter, A-9, B-1
IPXCP, 2-4
ISDN-B channel, 2-13, 2-14

L

LCP renegotiating, 3-3, 3-16
LCP. *See also* link control protocol
leased line, 2-12
Line Lists window, A-13
line parameters, A-13
  configurable with BCC, 3-14
line statistics
  calculating and viewing, 3-42
Lines button, A-13
link
  establishing, 2-5
  logical communications line, 2-13
  routing using PPP, 2-4
link configuration packet, 2-5
link control protocol
  definition, 2-5
  negotiations, configure-ACK, 2-6
  negotiations, configure-NAK, 2-6
  negotiations, configure-reject, 2-6

link control protocol (continued)
negotiations, configure-request, 2-5
renegotiation, 3-3
link control, enabling, 3-17
link maintenance packet, 2-5
link monitoring, 2-20
setting parameters, A-21
link quality
inbound, 3-33
inbound and outbound, 2-20
outbound, 3-33
link quality monitoring, 2-20, 3-31, 3-32
Link Quality Protocol parameter, 2-3, 2-20, A-21, B-2
link quality report, 2-20, 3-31, 3-32
period, 3-33
timekeeper, 3-32
link termination packet, 2-5
LINKQR, 2-20
LN, 2-13
local authentication protocol, 3-24
Local Authentication Protocol parameter, A-18, B-2
local name
CHAP, 3-30
local PAP ID, 3-27
Local PAP ID parameter, A-19
Local PAP Password parameter, A-19
loopback
detection, 3-38, A-27
disabling detection, 2-25
LQM. *See* link quality monitoring
LQR Reporting Period parameter, 3-33, A-22, B-3
LQR. *See* link quality report
LTSS Name encryption parameter, 3-13
LTSS Value encryption parameter, 3-13

M

Magic Num Disable parameter, 3-38, A-27, A-28, B-3
map, async control character, 2-24, 3-36
Max Configuration Failure Count parameter, A-17, B-2
Max Configure-Requests parameter, A-16, B-2
Max Terminate-Requests parameter, A-16, B-2
MCT1/MCE1, 2-14
media, multilink, 2-14
MIB objects, C-1
Mode Protection Key encryption parameter, 3-13
modem control character, 2-23
map, 2-24, 3-36
modem, asynchronous, 2-23, A-26
modifying interfaces, 1-3
monitor
link quality, 3-31
monitoring
congestion, 2-13, 2-15
link quality, 2-20
PPP links, 2-20
MRU
compatibility with CLAM and earlier versions, 3-39
MRU Size parameter, A-28, B-3
multiline, 2-12
comparison with multilink, 2-17
protocol prioritization, 2-17
specifying, A-12
multilink, 2-12
circuit (figure), 2-14
comparison with multiline, 2-17
configuring, 2-15, 2-16
endpoint discriminator, 2-3
media, 2-14
packet fragmentation, 2-16
protocol prioritization, 2-17
resequencing packets, 2-16
specifying, A-12
statistics, 3-42
using, 2-13
Multilink Fragmentation parameter, A-12, B-2

N

NCP. *See* network control protocol
negotiated IPX network number, 3-5
negotiating network layer protocols, 2-9
NETarchitect, starting, 1-3

network connection
negotiating, 2-9
PPP, 2-2
network control protocol, 2-2
disabling, 2-25, 3-13
network control protocol (NCP)
disabling, 2-25
network layer, 2-2
network security, 2-3, 2-8

O

Open Systems Interconnection, 2-4
OSI, 2-4
OSI Enable parameter, A-3, B-1
OSI Network Layer Control Protocol, 2-4
outbound link quality, 2-20, 3-33
Outbound Link Quality parameter, A-23, B-3
out-of-sequence packets, 2-16
overview, PPP, 2-1

P

packet
fragmentation, 2-16
minimum size for fragmenting, 2-16
out-of-sequence, 2-16
resequencing, 2-15, 2-16
PAP, 2-3, 2-8, 2-11, 3-24
customizing, 3-26
setting parameters, A-18
use with dial services, 3-26
PAP ID
identification mechanism, 2-11
local, 3-27
remote, 3-28
PAP parameters
Enable PAP Fallback, A-21, B-2
Local PAP ID, B-2
local PAP ID, A-19
Local PAP Password, B-2
local PAP password, A-19
Remote PAP ID, A-20, B-2
Remote PAP Password, A-20, B-2
PAP password
local, 3-27
remote, 3-28
PAP reject
allowing, 3-29
parameter descriptions, A-1
Password Authentication Protocol (PAP), 2-8, 2-11, 3-24
setting parameters, A-18
peer
definition, 2-13
IP address, 3-4
Peer Link Quality Report Timer parameter, A-22, B-2
physical media, multilink, 2-14
Point-to-Point network connection, 2-2
point-to-point protocol (PPP), 1-1
PPP
concepts, 2-1
configurable functions, 1-2
customizing, 3-1
data compression, 2-22
definition, 1-1
deleting, 1-6
disabling and re-enabling, 1-5
encapsulated frame, 2-10
initializing on an interface, 2-5
multiline, 2-12
multilink, 2-12
parameter descriptions, A-1
services, 1-2
show ppp commands, D-1
starting, 1-1, 1-4
statistics, C-1
PPP Interfaces window, A-13
PPP Line Lists window, A-13
PPP line parameters
configurable with BCC, 3-14
customizing, 3-14
PPP Mode parameter, 2-15, 3-11, A-12, B-2
prioritization
protocol, 2-17
product support, xx
Promiscuous synchronous line parameter, 2-24

protocol
data link control, 2-3
network control, 2-2, 2-4
protocol prioritization
definition, 2-17
multiline and multilink, 2-17
protocol-reject packet, 2-5
publications, Bay Networks, xix

Q

quality monitoring and reporting, 2-20

R

Raise-DTR modem, 2-14
receive percentages
calculating and viewing, 3-42
re-enabling PPP, 1-5
remote address, setting, 3-4
remote AppleTalk node number, 3-6
Remote AppleTalk Node parameter, A-9, B-1
Remote IP Address parameter, A-8, B-1
remote PAP ID, 3-28
Remote PAP ID parameter, A-20
remote PAP password, 3-28
Remote PAP Password parameter, A-20
remote peer
IP address, 3-4
renegotiating LCP, 3-3, 3-16
resequencing packets, 2-15
restart timer, 3-18
Restart Timer in Seconds parameter, A-15, B-2
RFC1661 Compliance parameter, A-28, B-3
RFCs relevant to PPP, 2-16, 2-25
routing over a PPP link, 2-4
routing table management protocol (RTMP), 3-6

S

Seconds between Xmit of Echo-Request parameter, A-15, B-2
secret, CHAP, 3-30
Service synchronous line parameter, 2-24
setting remote address, 3-4
show ppp commands, D-1
single-line (Normal), specifying, A-12
Site Manager, starting, 1-3
starting configuration tools, 1-3
starting PPP, 1-1, 1-4
statistics, C-1
calculating and viewing, 3-42
multilink, 3-42
support, Bay Networks, xx
switched line
dial-up line
PPP support, 2-10
synchronous connection, 2-23
synchronous line parameter
BOFL, 2-24
Promiscuous, 2-24
Service, 2-24
WAN Protocol, 2-24

T

T1 DSO, 2-13
technical publications, xix
technical support, xx
terminate-ACK packet, 2-5, 3-21
terminate-request packet, 2-5
maximum, 3-21
text conventions, xvi
threshold, 2-13, 2-20, 3-18, 3-31, 3-33
traffic
congestion monitor, 2-15
load balancing, 2-15
transmission parameters, 3-18

U

unnumbered interface, 3-4
using PPP multilink, 2-13

V

V.25bis modem, 2-14
V.35, 2-14
VINES Enable parameter, A-6, B-1
VINES Network Control Protocol, 2-4
VINES support, enabling, 3-8
Virtual Networking System (VINES), 2-4

W

WAN, 2-22
  data paths, 2-12
WAN Protocol synchronous line parameter, 2-24
wfPppCircuitEntry MIB, 3-42, A-2
wfPppCircuitMaxBuffers, 3-42
wfPppCircuitMaxLinks, 3-42
wfPppCircuitMlFragPerm, 3-42
wfPppCircuitMlFragTriggerSize, 3-42
wfPppLineEntry MIB, A-13
wfPppMlStatsAvgTxListLen, C-1
wfPppMlStatsBundleSpd, C-1
wfPppMlStatsCalcPercent, C-2
wfPppMlStatsCircuitID, C-1
wfPppMlStatsEntry MIB, 3-42
wfPppMlStatsExceededBufferMax, C-2
wfPppMlStatsHomeSlot, C-1
wfPppMlStatsLineCnt, C-1
wfPppMlStatsLinkIdleEvents, C-2
wfPppMlStatsNumPktsFragmented, 3-42, C-2
wfPppMlStatsReasmBufferMax, 3-43
wfPppMlStatsReasmFails, 3-43, C-1
wfPppMlStatsReassmBufferCnt, 3-43, C-2
wfPppMlStatsReassmBufferMax, C-2
wfPppMlStatsReSeqBufferCnt, 3-42, C-2
wfPppMlStatsReSeqBufferMax, 3-42, C-2
wfPppMlStatsRxOctets, C-1
wfPppMlStatsRxPkts, C-1
wfPppMlStatsSeqNumberArrivedLate, C-1
wfPppMlStatsSeqNumberLost, C-1
wfPppMlStatsTxOctets, C-1
wfPppMlStatsTxPkts, C-1
wfSyncEntry MIB, 3-43
wfSyncMtu, 3-43
wfSyncRejectsRx, 3-43
wfSyncRejectsTx, 3-43

X

Xerox Network System (XNS), 2-4
Xerox Network System Control Protocol (XNSCP), 2-4
XNS Enable parameter, A-4, B-1